ctc technology & energy

engineering & business consulting

Network Resiliency and Security Playbook

Prepared for The National Institute for Hometown Security
November, 2017

Columbia Telecommunications Corporation

10613 Concord Street • Kensington, MD 20895 • Tel: 301-933-1488 • Fax: 301-933-3340 • www.ctcnet.us

Contents

Figures

1 Executive Summary

This Playbook was written to help local and state governments adopt best practices for preventing significant communications infrastructure failures and stopping or mitigating intrusions, hacking, and other disruptions of communications networks.

The target audiences for this Playbook include information technology (IT) leaders and staff—the government employees who are responsible for implementing, operating, and maintaining IT systems—and the users of those government networks, including first responders. Because these audiences have a range of IT knowledge and expertise, this document includes high-level introductory information and links to useful background resources, as well as detailed technical descriptions of best practices.

1.1 Methodology

The National Institute for Hometown Security (NIHS), under a contract with the Department of Homeland Security's Office of Infrastructure Protection (DHS/IP), commissioned CTC Technology & Energy (CTC) to research and write this Playbook.

CTC's engineers and analysts prepared this Playbook in summer and fall of 2017, drawing on our independent research and our experience designing and engineering resilient and secure communications infrastructure for public sector clients nationwide.

1.2 Local and State Government Networks Are Targets for a Range of Reasons

This Playbook addresses some of the key reasons that local and state government entities need to routinely include security and resiliency in their infrastructure development processes:

- Local governments are attractive targets for cyber threats because they are often easy targets—especially those that do not have sufficient security resources and expertise

- Local government networks can also be attractive targets in their own right, given their maintenance of sensitive data such as tax and voter rolls, contracts, procurements, traffic data, public-run utilities, etc.

- Smaller governments often experience difficulty funding and staffing critical IT functions; as a result, those local governments might delay updating systems and applications, or even patching known issues, due to worry about proper functioning of legacy systems and risk of unintended impacts

- Poor or inadequate segmentation of government networks can lead to large impacts from modest intrusion efforts

- Local governments' networks are increasingly interconnected with other systems, including those of other local governments, federal agencies, and private sector partners
- Ransomware attacks make *any* target attractive regardless of size or sensitivity of data
- Storms, floods, and other natural threats are a constant concern for any network, but especially for mission-critical public safety and government communications networks

1.3 Network Resiliency and Security Require a Multilayered Approach

The concept of resiliency most commonly refers to network redundancy and diversity used in ways to avoid service interruption. These approaches typically relate to mitigating physical damage or failure of various network resources that would otherwise result in the interruption of critical processes and systems. But resiliency can also relate to the avoidance of logical failures and damage.

In 2013, the National Infrastructure Protection Plan (NIPP) developed a risk management framework for existing critical infrastructure that provides a useful starting point for developing a risk-management process at the pre-deployment phase.[1]

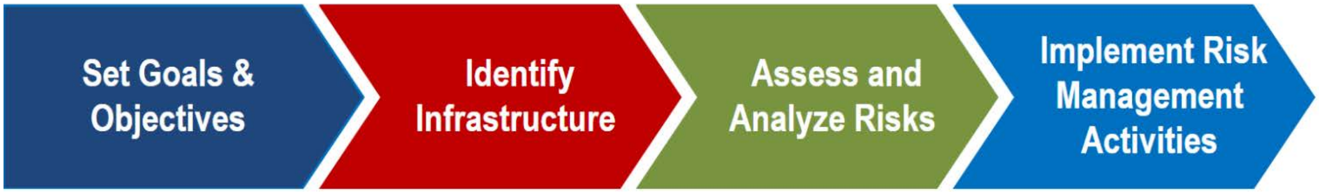
The NIPP's framework begins with setting goals. While it is certainly best practice to set goals and objectives, the reality is that many jurisdictions adopt vague, unspecific policies to address risk. Ideally, goals and objectives would be incorporated into a jurisdictional business continuity or disaster recovery plan that determines which critical systems need to be prioritized, with what resources and tools, and in what manner.

From a *pre-deployment* perspective, the goal is to implement an infrastructure that enables an effective risk-management framework and reduces actual risks and impacts. Specific goals and objectives may revolve around prioritizing public safety sites and systems, core networking, communications, and applications-sustaining infrastructure, as well as enterprise systems involved in government response and recovery operations.

Below is a modified process map showing example activities across the physical, network, cyber, and resource dimensions. While measuring effectiveness is a critical component of a continual lifecycle, it is not relevant at the pre-deployment phase. For simplicity, we are therefore omitting these activities from the pre-deployment phase.

[1] "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience," U.S. Department of Homeland Security, https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience, accessed November 2017.

Figure 1: Risk Management Process Map for Physical, Network, and Cyber Dimensions



Set Goals & Objectives

- Identify critical data and communications functions
- Set goals and prioritization for continuity of those functions

Identify Infrastructure

- Define architecture – physical, network segmentation
- Define critical assets
- Define critical network and segmentations
- Define critical sites and links
- Define critical staff and contracting resources

Assess and Analyze Risks

- Identify common sources of risk
- Identify gaps and vulnerabilities
- Identify single points of failure

Implement Risk Management Activities

- Adopt information and risk disclosure checklists
- Develop monitoring systems, and skilled staffing to mitigate risks
- Develop processes to support implementation of standards
- Incorporate security and resilience into procurement evaluation process
- Incorporate standards and risk disclosures into RFP process
- Set standards: develop levels of service, engineering standards, policies

We have expanded this framework, focusing on integrating resilience and security in every phase. Appendix A develops this framework further, including our key considerations for each, and references this Playbook for more information on each topic.

1.4 Jurisdictions Nationwide Demonstrate Exemplary Practices

From small towns to regional consortia to statewide deployments, local and state governments nationwide demonstrate best practices for network pre-planning, implementation, and management. This Playbook includes detailed case studies in Section 4, walking through the process each locality used, based on the above process map in the following examples:

NCRnet: The National Capital Region Interconnection Network, or NCRnet, is a public safety-oriented network that interconnects more than 20 jurisdictions in the Washington, D.C., metro area. As NCRnet was conceived and developed, the lessons of 9/11 for interoperability and resilience of voice communications were driving many concerns on the public safety radio side. But the region also foresaw the need for developing similar resilient infrastructure on the network side. These requirements were developed as part of the concept of operations and included the need for the network to be cost-effective, both in terms of capital and maintenance expenses; the network had to be financially sustainable in the long run, given that it would be maintained by the participating jurisdictions.

In addition, to meet the public safety mission, the network needed to be high-capacity, high-security, and high-availability. High availability meant that it needed to be largely independent of commercial networks. The concept was a private network that would work exactly when commercial networks would be congested or unavailable, such as during regional events. And, unlike commercial networks, NCRnet would give priority to public safety and emergency response related traffic.

The network needed to be flexible—able to support any type of application—and scalable, so it could add new partners. It also needed to allow for changes in configuration as needed to meet specific network requirements. And it had to be future-proof—capable of meeting future bandwidth and technological needs without the need for a complete redesign of the network.

Arlington County, Va.: Arlington County has operated a County fiber optic network since the late 1990s, when the County negotiated with the cable operator for dark fiber connectivity to approximately 80 government, school, and library locations. Several years ago, the County saw that this cable operator-provided fiber network would be inadequate to meet the County's future needs—not only in terms of number of strands, and the limited ability to negotiate a solid fiber performance SLA from the cable operator, but also as it anticipated that the cable operator would be unwilling to expand, augment, or properly maintain the network. Additionally, the County recognized its need and desire to have the full flexibility of its own fiber network to support economic development and partnership objectives that were not permitted under the terms of the cable franchise agreement.

The County is in the process of completing the construction of ConnectArlington, using County-owned fiber to replace the fiber supplied by the cable operator, and has almost entirely migrated away from any cable operator-owned hub sites or fiber.

Fairfax County, Va.: Fairfax County operates an extensive 430-site fiber network known as the I-Net network that connects the majority of government facilities and schools. Using dark fiber negotiated from the two cable companies in its footprint, and electronics operated by Fairfax County Department of Information Technology (DIT), the network became fully operational in 2006.

The network has a diversely routed backbone that mostly mirrors the Cox network backbone. County hub facilities are collocated with the Cox backbone, with the addition of the Fairfax Government Center as a major hub site. The County operates a multiprotocol label switching (MPLS) network with a dense wavelength division multiplexing (DWDM) backbone. The network serves county government and Fairfax County Public Schools (FCPS) sites.

Town of Holly Springs, N.C.: In recent years, the Town has made great strides towards facilitating ubiquitous and robust network and broadband connectivity and IT services, both internally and among the Town's businesses and residents, while maintaining strong controls over security and the ability to reliably deliver services.

The Town now operates and maintains its own fiber network, which spans nearly twice as many route miles as originally planned. The network provides extensive physical path diversity for connections between critical Town facilities, as well as redundant connections to outside networks and service providers. Backbone connectivity for public Wi-Fi, water and sewer utility systems, and traffic signal controllers are a few of the expanded roles of the Town's network today.

Commonwealth of Kentucky: The Commonwealth of Kentucky began planning a $270 million statewide, multipurpose, public safety-grade fiber optic network in 2013. The Next Generation Kentucky Information Network (NG-KIN) project (later renamed KentuckyWired) started as an initiative of former Governor Steve Beshear to address serious problems with the quality and availability of basic communications and broadband throughout the state. It is the most ambitious network of its kind, designed to eventually connect 1,026 government facilities, schools, and libraries; reach all 120 counties in a rugged, spread-out state; and become the core of Kentucky's mission-critical communications systems. Construction is currently underway with completion scheduled for 2022.

From the outset, the Commonwealth centered its needs assessment and planning efforts around technical, policy, and financial decisions. This process determined the extent and character of users' needs, engaged the stakeholders, and in the end delivered accurate cost estimates and risk assessments. These in turn enabled the Commonwealth to consider and evaluate a wide range of alternatives—technical, business model, operational model, and governance.

1.5 Issues for Future Consideration and Next Steps

While state and local government network planners cannot anticipate all circumstances or afford to harden all infrastructure, best practices for resiliency and security such as those outlined in this report are critically important. These include:

- Ensuring that your strategic planning process takes into account resiliency and security

- Building segmentation and resiliency into infrastructure
- Making decisions based on lifetime costs
- Ensuring you hire and train the appropriate staff (i.e., if possible, hire staff who have significant experience with similar infrastructure)
- Keeping the information security function separate from IT
- Training for emergencies—both internally (in the department and in the government) and with the surrounding region
- Working regionally—develop formal or informal consortia for information sharing, joint procurement, best practices, joint exercises and training

Applicants for DHS and other funding should comply with a checklist including all the above and establish baseline requirements for resiliency, cybersecurity, interoperability. Many of these are already included in *Fiscal Year 2017 SAFECOM Guidance on Emergency Communications Grants*.[2]

A state also typically has sufficient scale to make a significant difference in resiliency and security, especially if supported by funds and guidance from the federal government. A state can work with state universities to encourage and pay recently minted information security majors to work in underserved areas, for example.

The federal and state governments should continue to encourage and, where necessary, jump-start regional efforts.

Finally, infrastructure initiatives developed under the White House's infrastructure plans should also include, as appropriate, communications infrastructure. The classic example is to include communications conduit and fiber alongside new or repaired roads and bridges, which can be installed at a small percentage of the cost of building that infrastructure as a standalone initiative.

[2] "Fiscal Year 2017 SAFECOM Guidance on Emergency Communications Grants," U.S. Department of Homeland Security, Office of Emergency Communications, https://www.dhs.gov/sites/default/files/publications/FY%202017%20SAFECOM%20Guidance%20for%20Emergency%20Communications%20Grants_060717_FINAL508_0.pdf, accessed October 16, 2017.

2 Risks to Network Resiliency and Security

Local governments perform critical functions. These vary from community to community, but always include maintaining public safety and responding to emergencies through police, fire, emergency management services, and 911 systems. Most communities also have some role in providing utilities—water, sewer and sometimes power. Many also manage traffic (now including signal controls and cameras) and public transportation. Disrupting any of these functions can create cost and harm, or even death.

Each of these functions is increasingly tied into IT, requiring uninterrupted operation of computers, networks, and communications. Even if there is no emergency or threat, it is a significant challenge to ensure that all hardware and software continues to work, owing to the complexity of systems and the rapid changes in the way they are used. When the system is put under stress in an emergency, each component becomes even more critical, and people and systems sometimes must work harder and differently than in their day to day routine—and procedures and infrastructure need to be able to scale and cope. And if a dedicated attacker or emergency targets a system, there need to be:

- Procedures and precautions to guard against attack,
- Systems to block attackers,
- Systems to detect attack and intrusion,
- Procedures to backup and restore compromised systems, and
- Redundant systems and plans to work while the primary system has failed[3]

Risk can appear in the humblest corners of infrastructure. It is important to identify the risks to power and water at key facilities. Backup generators need servicing, regular maintenance, and routine testing, and must be properly sized for the electrical load of the network and data systems they support. A local government may need to weigh the additional cost of complexity of having generators away from ground level if there is likelihood of flooding.

Likewise, segmentation and separation of different types of communications that are intended for different levels of sensitivity, or that need to be kept from public view are mandatory for a resilient system. Again, cost tradeoffs exist, and there are many sound technological solutions that create this type of separation without having to necessarily create duplicate networks or resources—these include virtual separation along a transmission path by having separate communications in separate colors of light or separate communications channels within a medium. It may also include use of services from multiple service providers at once, or backup with wireless technologies.

[3] Please see Appendix G for a sample internal operating procedure that address these topics.

In all cases, it is incumbent on the government to understand the benefits and limitations of the available solutions, to look "under the hood" at the specifics of what commercial network providers or hardware or software providers are proposing, and properly specify the services as described in Sections 3.3 through 3.5.

2.1 Local Governments Are Often Easy Targets for Cyberattacks

Local governments are storehouses of critical and sensitive information. To perform their roles, they hold sensitive personal identifying information of residents and businesses. They handle tax information, procurement information, and information related to police and public safety procedures and operations. With the increase of "smart city" devices and applications, they have a view of many critical places and systems throughout their boundaries and accumulate increasing stores of data every day. The information needs to be guarded where it is stored, the information needs to be guarded as it traverses networks, and the devices that gather and process the information need to be secure.

It is incumbent on the local government to understand the areas of risk in its infrastructure and systems and to mitigate them as much as possible. Understanding the risks is possible, reasonable, and central to the message of this report. Risk mitigation is often a tradeoff with the available resources, but can be accomplished intelligently if best practices are used. For best practices in physical security and resilience, see Section 3.3; for best practices in network security and resilience, see Section 3.4.

2.2 Preparation and Protection from Storms, Floods, and Other Threats

Given the criticality of information and connectivity, networks and infrastructure need to be available both during and after emergencies including severe storms, floods, fire, and extensive power outages. Because it is not affordable to provide the highest resiliency and service hardening in all places at once, it is typically necessary to prioritize the most critical and valuable infrastructure and staff. Prioritization should include local and regional emergency planners and managers, and should be refined through emergency exercises and after-action reports.[4]

From a practical point of view, a local government would prioritize key locations, staff and operations and provide multiple ways to connect—by building key facilities away from FEMA-

[4] See, for example: "Strengthening Regional Resilience through National, Regional, and Sector Partnerships: Draft Report and Recommendations," National Infrastructure Advisory Council, November 21, 2013, https://www.dhs.gov/sites/default/files/publications/niac-rrwg-report-final-review-draft-for-qbm.pdf, accessed November 2017. *See also:* "Final Report: 9-1-1 Service Gaps During & Following the Derecho Storm on June 29, 2012," Metropolitan Washington Council of Governments, http://www.mwcog.org/asset.aspx?id=pub-documents/ol5cV1420140324140229.pdf, accessed November 2017.

designated flood areas, in physically robust buildings, in locations where power is historically stable, and with redundant wired communications. There should be additional levels of backup, including regularly tested backup generators, and backup wireless and satellite communications. And there should be advanced planning with utility companies and suppliers of generator fuel, such as provisioning dual feeds from the electric utility to critical datacenter sites; establishing contracts for generator fuel supply; and coordinating with regional partners capable of serving as a backup to local planning efforts.

Interoperability is critical in large scale emergencies, where outside responders such as federal authorities, state responders, other local governments, and utility companies will need to be part of the response. One approach to interoperability is the new FirstNet network, becoming operational in late 2017, which is centered around the AT&T mobile broadband network and augmented by deployable cell sites at events and incidents. FirstNet is designed to be a national, interoperable solution available to both to first responders and secondary responders, such as transportation, public works, and utilities. However, FirstNet by itself is not a full solution, as it may not be available in the most remote areas and worst emergencies—in which case satellite or land mobile radio systems may need to be part of the solution. And, as a wireless solution, is also more limited in capacity than a wired solution. For more information on FirstNet, see Appendix B.

2.3 Local Governments Need to Be Interconnected with Other Systems

Adding to the complexity, local governments need to be interconnected with other entities. These include neighboring local governments, for coordination of public safety and other joint efforts; state governments, for public safety, transportation, judicial and other joint efforts; and the federal government, for public safety databases.

In emergencies and crisis events, there may need to be coordination between incident commanders—who are generally local—and a wide range of entities that may be remote, including FEMA, the FBI, utility companies, the Red Cross, the National Guard, the National Forest Service, the National Park Service, and private companies. Infrastructure which coordinates communication between these entities must be both secure and flexible.

2.4 Smaller Governments Often Experience Difficulty Funding and Staffing Critical IT Functions

Local governments of varying sizes must approach IT security and network resiliency from an appropriate scale. There are no one-size-fits all solutions to network security compliance and resiliency, and ultimately securing a network and enhancing its resiliency is a matter of finding the right mix of outsourcing, internal staffing, and partnerships.

Financial and political barriers to implementing appropriate IT security controls and building robust and resilient communications infrastructure are wide-ranging, but far too often are primarily rooted in a simple lack of available financial resources. IT professionals in any sector have experienced the unfortunate truth that “the network” tends to only get the attention it deserves when something is not working properly. Proactive attention to IT matters requires that the decision-makers are properly informed about risk and threat impact levels associated with IT systems – and it is the job of IT staff to make this happen.

Funding often becomes a significant barrier in building the ideal infrastructure or solution. As an example, a local government can have the most control and security over its own network if it builds, owns, and controls its communications infrastructure, and if this solution has a mesh of separate and diverse physical paths between all important locations—and if the local government has sufficient skilled staff to operate and sustain the network.

Such a comprehensive solution is often cost-prohibitive. Fortunately, there are typically other, more affordable solutions that can provide acceptable security and resiliency—involving eliminating or mitigating single points of failure by potentially using a mixture of government-owned and carrier-provided services, different levels of route diversity to different facilities, and mixtures of wireless and wireline solutions. For practical information on localities implementing government-owned and carrier-provided strategies, see “Implementing Risk Management Activities” (Section 4.1.5).

Finally, as in all parts of IT, local governments face challenges in finding, training, and retaining skilled staff to keep networks and IT both resilient and secure. Governments have addressed these challenges not only by investing in training and certification (see Section 3.2.3), but also by participating in and initiating collaborative efforts with the state government or consortia of local governments in a region, and also by outsourcing. For an example of the latter, see Section 4.5.

A government could jeopardize its operations and endanger the public if it continues to operate a system with insufficient trained staff, expired licenses, or lapsed security updates, or after the system is no longer supported by the vendor. Therefore, governments need to consider the lifetime cost of an initiative—which may, after a detailed analysis, lead to a different approach than one that focuses only on the upfront cost—and underscore the value of buying in larger purchasing groups, examining cloud solutions, and investing in robust connectivity infrastructure to underlie it.

This would involve estimating the projected useful life of the asset, and the cost of licensing, operations, maintenance, training, and migration. Electronics providers often provide quotes for turnkey operations that can provide an upper limit for capturing some of these costs. If unavailable, estimating 25 percent of capital costs for electronic equipment maintenance can be a useful conservative budgetary approach. Though each network component has a different useful life, general estimates are 25 to 60 years for conduit, 20 to 25 years for fiber optic cable, and 3 to 7 years for firewalls, switches, and routers. Optical circuit equipment such as CWDM and DWDM tend to have longer life spans.

2.5 Poor or Inadequate Network Segmentation and Redundancy Can Pose Threats

There are many approaches to keeping networks safe and resilient. One is to break the network into segments, based on level of trust, type of use, and user group. Using segmentation, users on the internet or public networks can be kept from accessing sensitive information, from accidentally or deliberately affecting network performance, or from damaging or manipulating devices on the network.

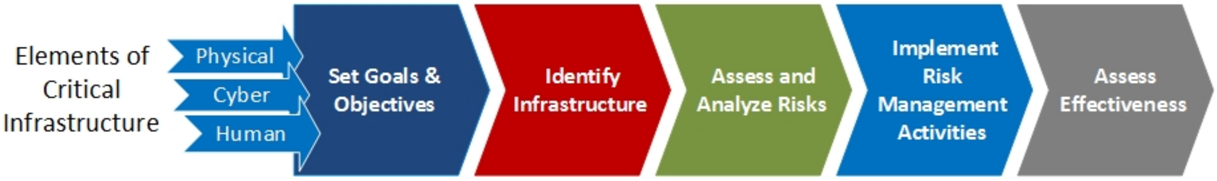
Segmentation techniques include virtual private networks (VPNs), in which communications on the internet or a private network share the same physical link, but are only readable or accessible by authorized users or connections to the network. They include virtual local area networks (VLANs) which set up separate channels within the same physical link that can guarantee specific performance as well as privacy. There is also wave division multiplexing (WDM) in which multiple signals of different colors travel simultaneously over the same fiber optic strand. And there is the capability to put different communications on different fiber optic strands in a cable—essentially creating an “air gap” between the communications.

These techniques each have their appropriate place, based on the needed security, cost, performance, and the available resources. This document describes the techniques in more detail and provides case studies as examples.

3 A Multilayered Approach for Security and Resiliency

In 2013, the National Infrastructure Protection Plan (NIPP) developed a risk management framework for existing critical infrastructure that provides a useful starting point for developing a risk-management process at the pre-deployment phase (Figure 2).

Figure 2: NIPP Critical Infrastructure Risk Management Process Map



The NIPP framework is generic, and applies to existing risk and cyber security practices. It may allow local jurisdictions to leverage existing processes to develop a pre-deployment framework for managing the security risks (both general and cyber-specific) related to fiber deployment.

We have expanded this framework, focusing on integrating resilience and security in every phase. Appendix A develops the below process maps further, including our key considerations for each, and references this Playbook for more information on each topic.

3.1 Enabling an Effective Pre-Deployment Risk-Management Framework

While it is certainly best practice to set goals and objectives, the reality is that many jurisdictions adopt vague, unspecific policies to address risk. Ideally, goals and objectives would be incorporated into a jurisdiction's business continuity or disaster recovery plan, which determines which critical systems need to be prioritized, with what resources and tools, and in what manner. For examples of best practices in this realm, please see the case studies in Section 4.

From a *pre-deployment* perspective, the goal is to implement an infrastructure that enables an effective risk-management framework such as the one outlined in Figure 2, and reduces actual risks and impacts. Specific goals and objectives may revolve around prioritizing public safety sites and systems, core networking, communications, and applications-sustaining infrastructure, as well as enterprise systems involved in government response and recovery operations.

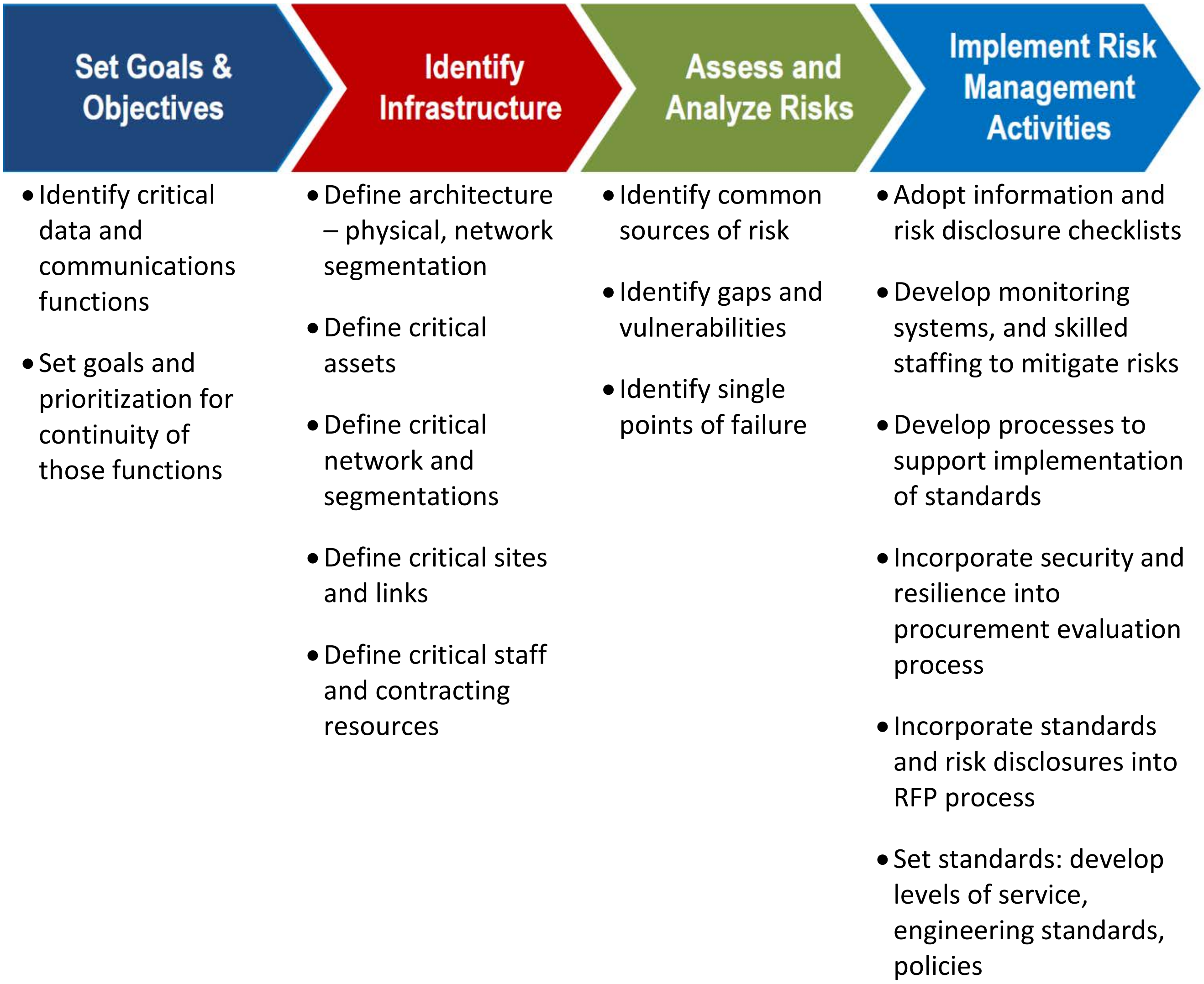
While measuring effectiveness is a critical component of a continual lifecycle, it is not relevant at the pre-deployment phase.[5] For simplicity, we are therefore omitting these activities from the pre-deployment phase. In addition, from a pre-deployment perspective, critical infrastructure is

[5] Evaluation metrics should feed into both the deployment activities in which quality and acceptance tests are conducted, and the post-deployment activities in which such metrics enter the regular risk management framework.

as much a question of definition as identification: pre-deployment activities involve determining how and where best to harden network infrastructure to manage risks.

Figure 3 is a modified process map showing example activities across the physical, network, cyber, and resource dimensions:

Figure 3: Risk Management Process Map for Physical, Network, and Cyber Dimensions



Set Goals & Objectives

- Identify critical data and communications functions
- Set goals and prioritization for continuity of those functions

Identify Infrastructure

- Define architecture – physical, network segmentation
- Define critical assets
- Define critical network and segmentations
- Define critical sites and links
- Define critical staff and contracting resources

Assess and Analyze Risks

- Identify common sources of risk
- Identify gaps and vulnerabilities
- Identify single points of failure

Implement Risk Management Activities

- Adopt information and risk disclosure checklists
- Develop monitoring systems, and skilled staffing to mitigate risks
- Develop processes to support implementation of standards
- Incorporate security and resilience into procurement evaluation process
- Incorporate standards and risk disclosures into RFP process
- Set standards: develop levels of service, engineering standards, policies

We have included an expanded version of this process map in Appendix A that maps to examples in this Playbook. The case studies outlined in Section 4 discuss how this process map can be employed, using real-world examples.

3.1.1 Incorporate Resilience into Every Layer

NIPP, in accordance with Presidential Policy Directive 21, defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions… [It] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[6]

NIHS, DHS, and private standards bodies have often advocated a generic and unified approach to managing natural and man-made risks. This all-hazards approach allows policy makers, executives, and managers to adopt a unified approach to intervention and risk management. This approach focuses on adopting good *processes* to manage risks rather than highly variable practices across deeply divergent threats, architectures, and organizations. At the same time, however, this approach means that practical recommendations and guidelines can seem vague or abstract, and can overlap both cyber security concerns and physical infrastructure issues.

From an incident-management and response level—which is the focus of most local government enterprises—situations that compromise the physical infrastructure require entirely different resources and responses as compared to cyber security-related attacks on the network. Moreover, physical or cyber security for local governments is often treated as secondary to the main business of government operations.

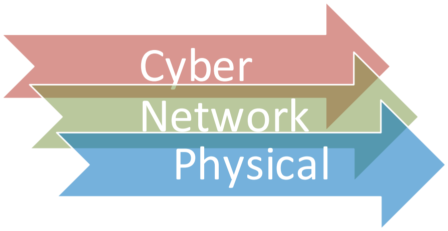
Focusing on resilience better aligns preparedness and response capabilities to the primary enterprise functions, which center around delivering network operations to the enterprise. As part of this task, continuity of operations, restoration of services, and the ability to both weather and recover from incidents are daily priorities built into regular operations and prioritized at the physical, network, and cyber layers. Given this, while incident management and expertise varies widely in terms of actual processes and roles in an organization, building resilience into a network must be a unified and multilayered effort.

For example, the ability to withstand risks, contain problems, and restore full operational functionality is often tackled through segmentation practices. Segmenting a network intersects the physical layer (including ring architectures), aggregation design, electronics, network provisioning, and cyber security designs. Building resilience, therefore, requires a coordinated approach at the pre-deployment phase in ways that specific incident response may not.

While this depiction of the various aspects of infrastructure is useful for a risk management framework that seeks to remind users to also take into account "human" factors, from a broadband network perspective, it may be more useful to layer dimensions that more accurately reflect typical divisions of labor in an organization (Figure 4). These divisions—namely physical (Section 3.3), network (Section 3.4), and cyber (Section 3.5)—should be analytically distinct.

[6] "Presidential Policy Directive—Critical Infrastructure Security and Resilience," The White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed October 2017.

Figure 4: Network Infrastructure Layers

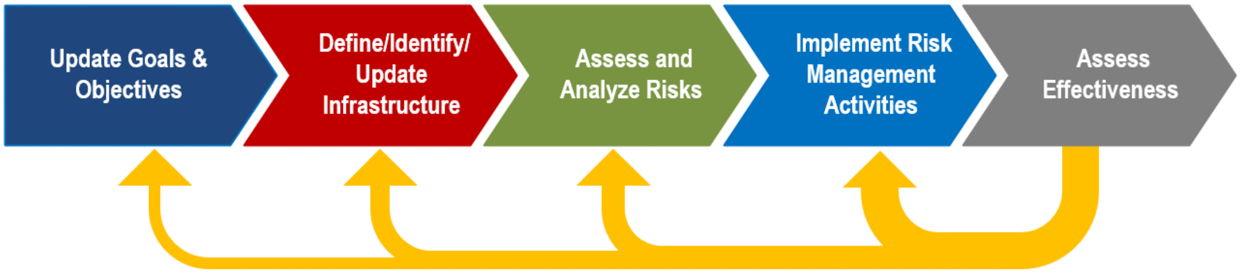


This approach better captures actual dynamics in smaller jurisdictions, where the cyber and network resources are not distinct, and where at least some of the physical infrastructure may be under the auspices of the network team as well. Given this, a lot of resilience that pertains to adaptation and restoration capability depends on the network layer, whether in regard to self-healing ring designs, segmentation of policy domains, electronic failover, load balancing, secure peering with other networks, or other network layer strategies.

3.1.2 Post-Deployment Considerations for Hardening, Resilience, and Security

In actual practice, jurisdictions seldom deploy a new network from scratch. Continual review and modification is therefore necessary (see Figure 5), which requires systems for measurement. Any expansion of the network or redefinition of critical systems or objectives will require updates not only to expanded or redefined activities, but also to risk assessment and management activities.

Figure 5: Continual Post-Deployment Cycle


Update Goals & Objectives
Define/Identify/ Update Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness

For example, requirements to support higher speeds over longer distances over the same fiber strands will require an update of objectives, network architecture, and fiber design specifications, splicing protocols, testing protocols, and benchmarks. Likewise, physical changes to the network (e.g., adding police stations) or new policy requirements (e.g., traffic segmentation for biometric applications that interconnect with federal systems) may require updates through the risk management lifecycle framework. This post-deployment assessment, illustrated with examples in Figure 6, will inform a locality's re-assessment of the first four phases of the risk management process.

Figure 6: Post-Deployment Assessment

- Perform network policy auditing
- Perform penetration testing
- Perform quality assurance/cable inspections
- Review major events and assess gaps
- Review NOC and SOC metrics for outages and incidents

Because hardening is often a practical matter of cost-benefit analysis, opportunities for hardening may be opportunistic—either as the cost-benefit calculus evolves, or as executive stakeholders' risk appetites change. For example, flooding events in other jurisdictions may make executives more receptive to investing in flood-mitigation strategies such as elevating and securing network equipment against flood damage, adding backup power generation, or setting aside funds for incorporating diverse fiber entry into key facilities.

3.2 High-Level Methodology

It is imperative that local government IT departments lead—or at least be aware of—the technology programs implemented by all other relevant government organizations to avoid any duplication, problems with support, problems with interoperability, or problems with managing security. This could be accomplished through formally putting any new or existing programs or initiatives under the auspices of IT, or by establishing a clearinghouse process under which any IT effort requires thorough and thoughtful review and approval.

Jurisdictions are often best-served by increasing the scale of any IT initiative. In these cases, a smaller local government can coordinate a jurisdiction-wide purchasing process of connectivity services, software, or devices that will facilitate the value of buying in larger scale. Efforts such as these often result in more attention from vendors, more participants in the procurement process, and more political support for the initiatives.

One effective strategy is to involve local schools, libraries, and municipal utilities in any IT initiative if they are not formally part of the government. In addition to increasing the scale of the effort, more funding options exist for solutions which address the concerns of these stakeholders. Additionally, participating in regional organizations like councils of governments or CIO groups will increase the government's sense of regional initiatives and ways to collaborate. Contact with local technical colleges and state universities will also further this goal.

If a government can create enough scale, it is always recommended that the security professional(s) be independent of the IT department, reporting separately to network management. Independence will lead to more secure processes both in IT and elsewhere.

3.2.1 Priority and Cost Tradeoffs

It is frequently difficult for any government to assess potential tradeoffs—especially regarding the security and resiliency of its assets. No local government believes it has enough funding to do what it needs to do, and there are many competing needs and threats among different departments. Any initiative must align with the priorities of the community—especially with any strategic planning the community has done. There are many local government priorities that may be addressed by building or improving networks:

- Public safety
- Education
- Economic development
- Transportation
- Upgrading public areas
- Improving broadband services
- Performance of local service providers

A local government should initiate IT strategic planning, if it has not already, being sure to include resilience and security in its analysis—both of what is being done now and how it plans to handle future needs. A local government which finds itself unversed in IT strategic planning would be best-served to educate itself through investment in and review of industry publications, such as those published by the Information Technology Infrastructure Library (ITIL) [7] and Control Objectives for Information and Related Technologies (COBIT), [8] both of which also offer certification programs.

ITIL combines service delivery with the functions required to support it, including sourcing analysis, contracts management expertise, security, and availability and capacity management. COBIT offers is an effective complement, helping to better organize and design business processes to facilitate value and better integrate risk management overall within the broader government enterprise.[9]

For any system or initiative, a local government must consider all alternatives, the various strengths and weaknesses of each approach, and a model of total lifetime capital and operational

[7] "ITIL," AXELOS, https://www.axelos.com/best-practice-solutions/itil, accessed October 2017.

[8] "What is COBIT 5?," ISACA, http://www.isaca.org/cobit/pages/default.aspx, accessed October 2017.

[9] Note that "resilience" is not a recognized category requiring management in these publications. Rather, resiliency falls between risk/security, capacity, and availability management.

costs. Understanding the total lifetime cost of an initiative is critical—including all maintenance, hardware and software updates, and training.

3.2.2 What to Staff and What to Outsource

Due to the increased complexity and costs of trained staff, server hardware, and software maintenance, and the relative decrease in the costs of connectivity and processing speed, cloud applications have become a better choice for many systems. Solutions including storage, disaster recovery, mail, office applications, mapping, and public safety applications have become effective tools for smaller enterprises.

If considering cloud services, localities must seriously assess the functionality of their systems in the event the provider or the local network fails, and the potential impact versus the cost benefits. There must also be an assessment of how to continuously improve network connection resilience and speed as needed, as well as a budget for those improvements—whether these services are purchased from a service provider or they are new infrastructure.

3.2.3 How to Get Training and Help

Local governments can work closely with area technical colleges and universities both to recruit graduates and to provide work-study opportunities for individuals in technology programs. Further, it may also benefit local governments to invest in certifying staff to accomplish their goals in-house.

The International Info System Security Certification Consortium (ISC2) offers the industry-standard Certified Information Systems Security Professional (CISSP) certification for staff with five years' experience in information security. The certification offers well-established training curricula and course offerings.[10] For staff with less experience, ISC2 also offers the Systems Security Certified Practitioner (SSCP) certification,[11] which requires less rigorous training in the same areas as a CISSP.

The SANS institute offers a highly technical certification, the GIAC Security Essentials Certification (GSEC), that has a greater focus on the technical (rather than management) realm.[12] The certification can be acquired through a six-day "boot camp," and is regarded in the industry as focusing on the necessary "street smarts" in information security.

[10] "Certified Information Systems Security Professional," $(ISC)^2$, https://www.isc2.org/Certifications/CISSP, accessed October 2017.

[11] "Systems Security Certified Practitioner," $(ISC)^2$, https://www.isc2.org/Certifications/SSCP, accessed October 2017.

[12] "Certification: GIAC Security Essentials (GSEC)," SANS Cyber Defense, https://cyber-defense.sans.org/certification/gsec, accessed October 2017.

The CERT Division through the Software Engineering Institute of Carnegie Mellon University has published the CERT Resilience Management Model (CERT-RMM) as "the foundation for a process improvement approach to operational resilience management."[13] Though the model does not address broadband/network resilience specifically, it does provide a generic framework that incorporates facilities, resources, and processes. For larger networks, it would benefit whomever is charged with this, be it the chief risk officer, security officer, or network architect, but in smaller jurisdictions it may very well fall to the CIO.

For those governments that have already implemented security and resilience plans, DHS's U.S. Computer Emergency Readiness Team (US-CERT) offers a Cyber Resilience Review (CRR), a no-cost, non-technical assessment of an organization's resilience in 10 domains:[14]

1) Asset Management
2) Controls Management
3) Configuration and Change Management
4) Vulnerability Management
5) Incident Management
6) Service Continuity Management
7) Risk Management
8) External Dependency Management
9) Training and Awareness
10) Situational Awareness

Each of these domains has an accompanying CRR Resource Guide developed for "organizations that have participated in a CRR, but are useful to any organization interested in implementing or maturing operational resilience capabilities for critical cyber-dependent services."[15] While the review consists mainly of interviews with key staff, organizations without comprehensive organization and knowledge will have the opportunity to mount a team effort to complete the review. CRRs offer an invaluable learning opportunity, and it would be in a local government's best interest to get leadership involved, especially as a sponsor and participant, along with any IT staff.

3.2.4 How to Build Resilience and Security into Infrastructure Planning

Localities anticipating deployment of new infrastructure must build resilience and security into the very design of the network, anticipating any potential problems before they arise. This

[13] "CERT-RMM," Software Engineering Institute, Carnegie Mellon University, https://www.cert.org/resilience/products-services/cert-rmm/, accessed October 2017.

[14] "Assessments: Cyber Resilience Review (CRR)," United States Computer Emergency Readiness Team (US-CERT), U.S. Department of Homeland Security, https://www.us-cert.gov/ccubedvp/assessments, accessed October 2017.

[15] "Assessments: Cyber Resilience Review (CRR)," accessed October 2017.

includes assessment of location risk, such as FEMA analysis of the flood plain, power feeds, and any history of power outages or flooding. If possible, these areas should be avoided for critical infrastructure, such as network hub sites.

Risk must be mitigated through a range of approaches—where the cost of failure is high, the need for diverse communications increases. Solutions to accomplish diversity include: dual-fiber routes, fiber plus a service provider (telco) backup or wireless backup, contracting both a wired service provider and a wireless service provider, or contracting with two separate wired providers (provided the providers have different routes for most of the path). Having a backup connection is more useful than a service level agreement (SLA) which generally has weak penalties that do not offset the cost of failure and generally have language that exempts flood and storm. For more information on this topic, see Section 3.3.2. For its practical applications, see the NCRnet case study (Section 4.1.2).

One main reason for infrastructure failure is of the loss of electrical power. Key sites should have a good history of power quality, with uninterruptible power supplies (UPS) for critical components, and backup power generation capabilities. Especially critical facilities should have redundant generators. As discussed in more detail in Section 3.3.4, local governments should make plans to ensure that sufficient fuel is available for generators at important network facilities; that materials are stockpiled for generator maintenance; and that redundancy of utility power corresponds to the criticality of the site. Fuel suppliers must be able to demonstrate how they are supplied and how they will continue to be supplied in and prioritize the service in a long-term emergency. Local governments should coordinate with state emergency management officials to assess fuel supply chain resiliency, and may even be able to use contract vehicles already in place for emergency fuel supply.

If deploying new infrastructure, a well-designed procurement process which clearly articulates the locality's infrastructure resiliency and security goals will leverage an engineering firms' ability to implement both of these attributes from the pre-deployment phase (see Appendix C).

Post deployment, localities can employ a variety of strategies to increase resiliency and mitigate risk. These could range from deploying additional infrastructure (which follows the best practices discussed in Section 3.3) to gradually upgrading infrastructure to meet these standards. If such strategies prove cost-prohibitive, localities can employ other tactics to mitigate risk on a network that is already deployed.

From a logical perspective, localities must employ well-developed and comprehensive network use and information security policies (see Appendices D and E), prioritize network segmentation, network segment intrusion detection and prevention, and robust identity management systems. Localities that wish to leverage the private sector's expertise can also employ robust cloud-based solutions for many applications which they cannot afford—or do not have the experience—to support locally.

To obtain a deep base of information from the vendors that supply network electronics, services, or staff, localities can develop a vendor questionnaire that assesses security practices and risk-management activities and standards adopted by its vendors. This allows localities to better assess risks when utilizing outside support, and implements resiliency planning in the initial phases of planning a new network component. (See Appendix F.)

Since a locality can implement these components without redeploying fundamental infrastructure, it is best to view network and cyber resiliency and security as an ongoing planning effort—continually assessing the system's effectiveness. By keeping abreast of industry standards and developments, and working with other localities to share practicable information and strategies to address ever-evolving network threats, a smaller jurisdiction can work to remain "ahead of the curve" in this realm.

3.3 Best Practices in Physical Security and Resilience

Security and resiliency of a network starts with its physical layer systems and underlying support infrastructure. These foundational components include the physical cabling, electrical power, environmental controls, and physical protection of the network electronics. At the design and implementation phases, the objective must be to ensure that sufficient redundancies and failover mechanisms exist to ensure continuity of operations when components fail or are damaged: Network resiliency is most commonly achieved through redundancy and diversity of physical network components employed in ways to avoid service interruption during any number of unplanned outages or events, in particular in relation to physical damage or failure of various network resources that would otherwise result in service interruption of critical processes and systems:

- **Redundancy:** Primary focus on having from (N+1) up to (2N) resources online to mitigate risk of service interruption in the event of equipment and/or network resource failure. Redundancy may be configured to run in normal mode as either active/standby or active/active (load balanced). At minimum, redundancy provides continuous service despite the loss of any (N) system or resource, while handling 100 percent of normal capacity, while repair or resolution is reached.

- **Path Diversity:** Most often an outside plant and circuit selection strategy—primarily protecting against physical damage impacting critical infrastructure, regardless if natural or man-made. Broader areas of impact (regional or national) are significantly more difficult to prepare for, as diverse paths may be equally impacted.

Operational considerations for network resiliency include: 1) implementing proper surveillance of critical infrastructure to identify failures; 2) ensuring provisions are in place to effect restoration activities; 3) maintaining processes to reduce the risk of damage to system components, and to periodically test their resiliency; and 4) maintaining accurate and sufficiently detailed documentation to support all maintenance and restoration activities. For an example of these considerations, see Appendix H.

3.3.1 Physical Site Access Controls

Uncontrolled access to physical network assets, in particular routers and other network electronics, can pose significant risks to network availability and application security. This is a risk presented either from accidental damage, cable disconnection, or misconfiguration, or from malicious attempts to disrupt the network or compromise data integrity or secrecy. Aside from causing physical damage to network electronics or cabling that might cause an outage to network services, gaining physical access to network routers by an individual with malicious intent can allow for relatively unsophisticated means to intercept data and/or modify device configuration passwords directly through physical console management ports.

To effectively mitigate this risk, site access must be controlled both physically and as a matter of policy. Sites housing network equipment should provide reasonable physical security in the form of locked doors, active intrusion detection and alarming systems, and ideally, electronic access controls and video surveillance that provide positive identification and logging of all individuals gaining access to the site. Policies should mandate logging of access to spaces containing network equipment, as well as specify methods for proper vetting of personnel (i.e., background checks and employment status) that are allowed unescorted access to network equipment.

3.3.2 Link Redundancy and Fiber Restoration

Outdoor physical cable plant is an exposed asset that is at risk of damage from a number of threats. Accidental damage to underground cable, whether directly buried or installed in conduit, can occur due to excavation and other underground construction activities occurring near the cable. While proper utility locating in accordance with State "one-call" center laws can help mitigate this risk, damage of this type is not uncommon. Cable installed on aerial utility poles, on the other hand, is more prone to breaks caused by damage to utility poles resulting from traffic accidents or bad weather, particularly as a result of trees falling onto these utility lines. Underground and aerial cables can be damaged by rodents and other animals that chew through cable. Malicious physical attacks are also possible, whether targeted or the result of random vandalism.

When network links are supported over "dark" fiber, whether owned or leased, the physical fiber path is general known to the fiber owner or lessee, which allows the risk of outage to be assessed more accurately, and risk mitigation strategies implemented more effectively. The impact of any individual fiber break can be contained by having in-house or contracted resources on hand to begin repairs within consistent timeframes established by SLA or maintenance contract terms. Actual repair timeframes in emergency situations should be expected to vary from a few hours to several days, depending on the severity of the damage and the corresponding circumstances that might strain repair resources, such as widespread damage due to extreme weather.

Leased network connections managed by commercial providers can be similarly "guaranteed" by contractual terms within an SLA, which may or may not meet the requirements of the applications they support, but are still prone to outages due to physical plant damage that is subject to real-world repair times. Target levels of link reliability may not be met in a disaster situation during which the network is most needed to support first responders and other emergency support functions, and financial damages associated with unmet SLA performance specifications are likely not sufficient to mitigate the impact of risks to the physical network. In the case of leased circuits, physical network attributes are generally unknown by the customer and considered proprietary by the network operator, which inhibits the customer's ability to effectively assess risks to network connectivity.

For critical network services, it is thus necessary for local governments to incorporate sufficient redundancies into their networks to minimize the risk of network outages caused by loss of physical connectivity. Physically diverse paths for connections between critical network sites coupled with network electronics configured for automatic path protection switching or load balancing between redundant connections can achieve near complete fault tolerance. Diversity can be accomplished through any combination of connections that are leased or owned, provided that they can be evaluated to ensure the physical paths are sufficiently diverse so as to be unlikely to be impacted by the same threat at the same time, whether an accidental or intentional incident. This type of physical diversity, where feasible, should extend to the indoor cable plant pathways through a network site to the fiber termination panel or similar demarcation.

Configuring network electronics to take advantage of diverse physical paths has never been easier, particularly when both links are supported over dark fiber offering end-to-end control of the network electronics used to activate the links. Standards-based Ethernet switches used in nearly all local government networks take advantage of redundant connections, generally by default, using Spanning Tree Protocol (STP) to identify the redundant links, shut down redundant connections to prevent unwanted "loops," and automatically reactivate these links when the primary path is interrupted. Similarly, routers can utilize dynamic routing protocols to achieve similar functionality with more rapid convergence over backup connections, particularly where a combination of private and leased network connections, such as virtual private networks (VPNs), are used to establish diversity. Where dark fiber connectivity is available, link aggregation can be configured so that load balancing over redundant links provides increased capacity and virtually immediate convergence in the event of a break. Regardless of the particular configuration and technology used, this type of link redundancy can reduce the impact of a fiber cut from days or hours to seconds or less.

3.3.3 Fiber Damage Prevention and Documentation

Preventing damage to outside cable plant is an important part of an overall strategy to mitigate the risks of physical network outages. If possible, hiring staff who have significant experience with the infrastructure, such as those who previously worked in engineering and construction locally with telecommunications operators, and have experience supporting networks bound by SLAs, will offer vital "real world" planning when deploying new infrastructure. If this is not possible, an efficient, thorough, and timely locating process can help prevent damage to the infrastructure.

Locating fiber optic plant accurately and quickly in response to utility locate requests (i.e., "811" tickets) helps ensure that construction activities in the local vicinity does not result in accidental damage. Whether performed by internal staff or contractors, processes must be in place to perform locates in accordance with applicable damage prevention laws. Maintaining accurate documentation of the physical plant can help locators perform this function more accurately, and particularly when maintained electronically in a GIS format, can be included in the construction plans for other capital projects more readily to facilitate proactive avoidance of potentially vulnerable fiber.

3.3.4 Electrical Power Supply Resiliency

A lack of electrical power resiliency is one of the more common causes of service outages for nearly any type of communications network. Network hardware generally requires well-conditioned electrical power, and in fact, power voltage fluctuations can reduce the mean time between failures (MTBF) of network hardware. Even a momentary power outage or significant drop in voltage can cause network hardware to reboot, incurring a few minutes of outage in many cases, or longer if resulting in a system crash or if system configurations are not properly restored upon a subsequent power-up. Ultimately, the impact can be equivalent to a hardware failure or fiber cut.

The risk of power outages can be reduced by working with the electric power utility to supply important network and datacenter sites with redundancy of utility power feeds. This can vary in complexity from dual feeds from a single electrical power substation to single or dual feeds from each of two redundant substations. The cost of any redundant utility power configuration will vary greatly from one location to the next, and must be designed and implemented by the electric utility operator. The degree to which this might be worthwhile depends somewhat on the robustness of local backup power systems and the resiliency of fuel supply chains required for corresponding local power generation.

Short-term power outages are common, even during mild storms, with aging public power infrastructure often susceptible to ice storms, wind-related damage, power demand spikes, and other disruptions. To reduce the risk of short-term power-related threats, Uninterruptible Power Supply (UPS) systems are generally sufficient. If properly maintained (i.e., batteries replaced every three to four years) and not overloaded, UPS hardware will effectively mitigate the risk of short-term outages and voltage fluctuations.

Longer term outages, although less common, pose a more substantial potential impact to the network, as backup power generation is generally required for outages lasting beyond more than a few minutes. Backup power generation is costlier, and the equipment requires rigorous maintenance and testing to reliably offer backup power. Generally, weekly tests under full load are considered an acceptable means for generator testing. Routine maintenance, from changing lubricating oil and filters to major overhauls, must be performed in accordance with manufacturer recommendations.

Moreover, sufficient fuel supply, particularly during large scale emergencies that strain public fuel supply chain infrastructure, must be ensured through fuel storage reserves or fuel service contracts with appropriate guarantees tied to suitable fuel storage and delivery resources. Local governments should take into account their fuel requirements for generators supporting critical network systems, and ensure sufficient reserves and/or supply contracts are in place to meet these needs in an extended outage situation, recognizing that larger scale disasters and weather-related incidents could impact utility power for a week or more.

Similarly, materials required for performing maintenance of generators during extended power outages (e.g., lubricating oil, fuel and oil filters, and common spare parts) should be stockpiled onsite. Generators fueled by natural gas, where available, may provide a mechanism for more reliable long-term fuel supply in certain types of emergency situations, as natural gas is generally supplied via a robust underground pipeline network as opposed to via tanker trucks on potentially flooded or congested roadways.

Generator redundancy should be considered for more critical sites, like datacenters; redundancy can generally be most cost-effectively implemented for these larger facilities with multiple smaller generators configured in parallel to meet the full power load requirement with a failure of any one generator. A local fuel supply should be maintained, whether liquid propane or diesel, that is sufficient to keep generator(s) running for as long as might reasonably be required for fuel delivery to occur. Generator redundancy may also provide a mechanism for fuel supply redundancy, with sites equipped with generators fueled by a combination of diesel, liquid propane, and/or natural gas.

3.3.5 Climate Control Resiliency

Proper climate control is critical for most network electronics to operate reliably. Most network electronics are not environmentally hardened, and as such, must operate within typical environmental ranges (i.e., 32 to 104 degrees Fahrenheit, 5 percent to 90 percent humidity, non-condensing). Datacenter and wiring closet temperatures can reach temperatures well above this typical range, even when outside temperatures are mild, simply due to the heat dissipation from the network electronics in a relatively closed environment with minimal circulation from external environments. Network equipment can reach critical temperature levels and begin to malfunction or shut-down in a matter of hours after the failure of air conditioning systems.

Network hardware should be located in spaces with HVAC systems capable of maintaining required environmental ranges, and should be implemented in redundant configurations when supporting critical network services. In the event of a failure of a non-redundant system, it may require more time to complete repairs than available before temperatures begin to impact network connectivity.

3.3.6 Network Electronics Redundancy

Network electronics, including switches, routers, and firewalls, represent an obvious potential point of failure for network connectivity. Aside from the physical diversity of actual network links, the network electronics and their internal components can be deployed in a redundant fashion to increase network resiliency where necessary to support critical services. A single edge router failure, for example, will reduce total annual network availability for a particular network site connected to a wide area network to approximately 99.9-percent availability (roughly 9 hours of downtime), or less, depending on the amount of time required to replace the failed component. Where the highest levels of availability must be maintained (i.e., 99.999-percent), network equipment must be deployed in a fully redundant hardware and link configuration (i.e., two routers, each supporting a discrete network connections).

Enterprise-class network equipment is available with redundancy of certain common components, even for edge devices in a network, such as redundant power supplies capable of supporting the entire system power load in the event one fails. Larger core network devices may have full redundancy of all common components, such as route processors, switch fabric, etc., or can be deployed in a “stacked” configuration with multiple individual chassis containing components that can support others in the same stack.

3.4 Best Practices in Network Security and Resilience

Beyond the physical components of a network's infrastructure, security and resilience must also be designed into the logical layer of a network. This can be accomplished through the implementation of hardware, software, policy, and application solutions—all of which must work together to protect the network against compromise of any sort. The following represent best practices in logical network security and resilience.

3.4.1 Information Security Policies

A jurisdiction's security policy must, by its emphasis, help to identify and protect the most critical systems and resources needed during crisis for survival. Policies must be well-written, make good common sense, and be easy to understand and follow. Policies should be regularly updated, and readily available for everyone to access. All users must read, acknowledge, and understand the written policy prior to receiving network or system access, and policy must be enforced at all levels within an organization.

If policies are not enforced, they can quickly become a set of optional guidelines. They must explain processes for notification of non-compliance. In cases of willful disregard, repeated non-compliance, or extreme negligence, the policies must include processes for disciplinary actions up to and including termination of access or employment. IT staff is charged with measuring and reporting on compliance. Disciplinary action requires executive support as this is owned by each division or department of an organization. Finally, to properly protect the organization, good policy should never require or allow special exceptions or waivers.

Common policies, such as locking computers after set periods of inactivity, restricting the use of personal devices on the network, and requiring strong passwords are likely to be unpopular controls among many non-IT staff within any enterprise. However, security of a local government's critical infrastructure and data should not be compromised by making IT security policy subject to the preferences of each stakeholder; rather leadership should empower IT management to set policy aligned with organizational goals, strategic input from stakeholders, and a sound business case, while requiring enforcement of these policies throughout the organization.

For an example of a robust information use and regulations policy, please see Appendix D. We have also included a sample data nondisclosure and security agreement in Appendix E.

3.4.2 Network Segmentation

Network Segmentation refers to techniques for helping to manage performance and security of IP networks. Network segmentation provides multiple strategic points within a network to enforce security policy with access rules between segments. By separating shared networks into smaller network segments, connections between these segments must pass through a network operating system, a router, and/or a firewall. These network devices can provide very effective control at the network level, and are used to technically both implement security and resiliency policy objectives and to enforce them.

Segmentation defines boundaries between groups of networked systems along criteria such as the sensitivity of information to which they have access, or the separation of business units within an organization. Access to each segment requires successful authentication and proper authorization to access the information or systems on that segment.

3.4.2.1 Segmentation Technologies

Network Segmentation can be technically achieved in several ways. Specific techniques to use largely depend on the level of security risk involved, and the availability of network resources to properly design, implement and support the selected method. More powerful techniques are also more technically complex and costly.

3.4.2.1.1 IP Subnets

IP Subnets offer the simplest option to segment IP networks into smaller IP networks (sub-networks, or subnets) that require a router or firewall to forward traffic between them. This is accomplished by subdividing the network portion of an IP address into multiple smaller IP networks. Subnets are very common and often required, but offer the least flexibility in terms of segmentation approaches.

3.4.2.1.2 Virtual Local Area Networks (VLANs)

Virtual Local Area Networks (VLANs) are a relatively simple, and commonly available feature in all Ethernet switches. Systems on a VLAN interact as if they are on a single physical LAN, regardless of the systems' physical location, de-coupling physical location from network location. By separating traffic and allowing access controls on shared network systems, VLANs are commonly used to segment networks along functional boundaries, such as departments in an organization (e.g., an "ACCOUNTING" VLAN may span across multiple cities or states to include all systems in all locations that belong to ACCOUNTING). VLANs require a router or firewall to forward traffic between one VLAN and another, and necessitate some planning and design, but provide increased flexibility

3.4.2.1.3 Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) is a powerful network technology, offering several methods for segmentation into Virtual Private Networks (VPNs). MPLS Layer-2 VPNs offer both point to point (referred to as pseudo-wire, emulating a circuit such as a T1), and point to multipoint (referred to as Virtual Private LAN Service (VPLS), emulating a switch or VLAN that connects systems on a shared LAN). MPLS Layer-3 VPNs can segment networks into Virtual

Routing and Forwarding (VRF) domains to provide an isolated and highly secure IP network environment

3.4.2.1.4 Dense Wavelength-Division Multiplexing

Dense Wavelength-Division Multiplexing (DWDM) is a best-practice technology for the highest-speed network routes and network backbones. Using a highway metaphor, these would be the "interstate" routes between the network hubs. These routes need to be fast, reliable, and able to accommodate sudden and unexpected increases in demand.

DWDM technology is virtual segmentation of a shared fiber strand. It increases security by eliminating the need to share network routers or switches, and IP address space. The separate interfaces on each side (e.g., local government, Public Safety, anchor institutions) are on completely separate channels from the other interfaces and the traffic does not use the same routers, switches, or addresses. This is the most secure type of separation, short of using entirely separate fiber strands, and makes it possible for a single fiber strand to carry internet traffic and secure public safety communications, sensitive health care information, and leased circuits from private sector service providers.

3.4.2.2 Common Functional Segmentation Boundaries

Segmentation can be technically implemented anywhere in a network. There are a few common practices and approaches (schema) to determining where to segment a network, in terms of defining the technical boundaries between segments. The specific schema to use largely depends on the level of sensitivity or information security risk involved, which places in the network are most efficient or effective for controlling access, and the availability of technical resources to properly design, implement and support the selected method.

The most common approach is to segment along functional network boundaries. This can be very effective, and requires minimal effort to implement using virtual local area networks (VLANs). Access permissions between VLANs can be enforced with Router Access Control Lists (ACLs) or a Firewall (see below). Functional segmentation can be highly effective in stopping or slowing down unauthorized access to segments of the network, and is generally considered to be minimal best practice.

Common functional boundaries include:

- User Access
- Real-time isolation of sensitive applications, such as: VoIP, VTC, CCTV
- "DMZ" for public-facing systems (DNS, Web, Email)
- Data Center networks
    - Storage area network (SAN)
    - Database servers

    - Critical applications / suites
    - Operations, Administration, and Management (OAM)
- Regulatory compliance
    - PCI-DSS (e-Commerce, payment systems for parking, permitting, fee collections, etc.)
    - HIPAA (medical insurance and healthcare records)
    - Other PII (Personnel records, HR data, Payroll and Finance, etc.)
- Intranet access
- Remote Access
    - Users
    - Vendors / Partners
    - Administrative
- Guest internet access network (Ethernet or Wi-Fi)
- Public Access networks (Public Wi-Fi, Libraries, etc.)

3.4.3 Network Segment Access Control

Network access control manages access to various segments of a network by ensuring that identity is properly authenticated, and the authenticated party is authorized to access the segment. Network devices on the boundary between network segments are used to implement access controls on a network level.

3.4.3.1 Switches

Network switches are found everywhere, but most commonly associated with the edge of a user network, and provide physical connection points for all systems connecting to the network. Switches define and implement VLANs. Systems connect (with a patch cable) to an assigned physical port on a switch, and that access port is configured to provide access to a particular VLAN.

3.4.3.2 Routers

A router is any network device that provides logical connectivity (routes traffic) between two or more IP networks. Routers communicate with other routers using routing protocols, to exchange information about networks they can reach. Basic routing can be provided by a server with multiple network interface cards, a network switch which includes routing capability, a dedicated appliance, or a firewall.

Most routers can support configured rulesets to control (permit or deny) certain types or classes of traffic between networks. A ruleset on a router is called an Access Control List (ACL). Routers can perform simple traffic inspection in real-time (at line rate), comparing each IP packet to an ACL ruleset, making the appropriate permit (forward) or deny (drop) decision. Router ACLs are similar (but generally less powerful) than firewall rules. While ACLs are very effective, the router is purpose-built to route IP traffic and is not best suited as a primary or solo security device.

3.4.3.3 Firewalls

A firewall is a network device that is configured with specific set of rules, and performs packet level inspection of all traffic to determine whether to permit or deny passage. The granularity of rules available in most firewalls, the speed at which they can inspect packets, and the difficulty of tricking the system is much higher than most routers. A firewall is purpose-built and hardened for security.

Firewalls may be deployed on the perimeter, or "edge," which is any external network boundary between trusted and untrusted networks. A firewall may also be deployed between trusted internal network segments. It is not uncommon for an organization to deploy many more firewalls protecting internal segment boundaries than perimeter network connections.

When deployed as perimeter firewalls, these devices often fill other important roles in addition to enforcing rules (ACLs). These additional roles are essential and critical to most operational networks. Next-generation firewalls include network intrusion detection systems (NIDS) and in many cases network intrusion prevention system (NIPS), discussed in Section 3.4.4.

3.4.3.4 Endpoint Security

User workstations and laptops have become the new "edge" of the network. Despite other controls in place, some exploits are still delivered to end user inboxes. In these situations, user training and awareness are proven to be highly effective. Nevertheless, email scams have become so pervasive, realistic, and highly personalized that it is unrealistic to place full responsibility on the end user. Strong endpoint security significantly protects end systems from all forms of malware, prevents intrusion and hijacking before it happens, and enforces security policy. It also protects the end user.

3.4.4 Network Intrusion Detection System

As the name suggests, a Network Intrusion Detection System (NIDS) alerts security operations of likely intrusion incidents, under pre-defined threat conditions. A NIDS may be implemented as a stand-alone appliance, network probe, or server-based software, or more commonly as a module in a next-generation firewall.

For known-threat recognition, a NIDS relies on a threat signature database. The system is usually subscribed to a live signature feed from the NIDS vendor or a third party. This live feed ensures up-to-date synchronization with a cloud service for new and emerging threat signatures. The effectiveness of NIDS against known threat signatures is extremely high.

A NIDS also uses a combination of dynamic techniques to detect undefined network intrusion attempts. This requires real-time monitoring of network traffic combined with scoring methods such as reputational analysis and anomaly detection, which leverage artificial intelligence and machine learning technologies.

Dynamic detection provides a layer of defense against unknown or mutating threats, but also carries some risk of false-positive results wherein legitimate traffic is reported as malicious. Detection sensitivity can be increased or decreased; finding a proper balance for each environment is critical to operational effectiveness. If detection sensitivity is too high, security operations may become overwhelmed by false alarms, and if too low, some threats may pass undetected.

3.4.5 Network Intrusion Prevention Systems

A Network Intrusion Prevention Systems (NIPS) uses detection methods and techniques similar to a NIDS. However, a NIPS provides an automated response capability to dynamically and proactively block detected network threats in real time. This is accomplished with dynamic firewall changes to block malicious traffic.

As with a NIDS, the sensitivity of dynamic detection techniques may be turned up or down. However, with NIPS a false-positive hit can have a significantly greater operational impact if the response includes blocking legitimate network traffic.

3.4.6 Identity Management and Authentication

Proper user authentication has far-reaching implications. User authentication is the first of several steps for determining what each user has access to, and what they are permitted to do with it once they have access. If user authentication processes can be tricked or subverted, the consequences can be severe. Authentication needs to be both strong and bulletproof.

3.4.6.1 Usernames / Passwords

The most common approach to authentication involves use of a username and a password. Usernames and passwords typically have system-enforced requirements for length and complexity. Passwords commonly have additional system-enforced rules for expiration and prevention of re-use.

Username and password rules need to be clearly included in a network's information security policy and enforced at a system level. Rules need to be carefully balanced to prevent users from needing post-it-notes to remember complicated passwords. The use of pass-phrases is highly recommended. These can be easy-to-remember long passwords (e.g., "My Favorite Car is a 1957 Chevy!") or perhaps used as a hint to remember a shorter, more cryptic acronym (e.g., "MFCia57C!").

3.4.6.2 Multi-Factor Authentication

Multi-factor authentication (MFA) includes the use of a username and password (i.e., "something you know") authenticated against a second factor—either "something you have" (e.g., a code sent to your cell phone, or a token) or "something you are" (a biometric scan).

MFA has become easy to implement and is extremely effective at improving the strength of user authentication. It is used for online banking and ATM access, countless cloud services, and common email platforms such as Google and Yahoo.

3.4.7 Cloud-Based Services

As IT becomes more complex, it has become more common to use centralized, external cloud providers to manage storage and operations of systems. This is a double-edged sword, enabling the most challenging functions to be managed by large, experienced entities with large economies of scale—but also taking those functions out of the sight and control of the government. This approach thus requires high levels of trust in both the cloud provider and in all the network and other resources needed to reliably and consistently connect to the cloud. There need to be procedures around the selection and management of the cloud services, as well as procedures to use in the event that a service or the connection to the service fails.

- **Information Security:** Many aspects of information security fit within the definition and/or scope of resiliency. Information Security is the business of protecting information from any risk of compromise in terms of the information's confidentiality, integrity, or availability.

- **Cyber Security**: Focus on prevention and detection of man-made attempts to exploit vulnerabilities to gain access to valuable systems and information. Some cyberattacks threaten to make information systems unavailable (e.g., ransomware). Preventing these attacks maps well to the notion of resiliency (continuous operation in the face of difficulties). Many other cyberattacks seek to extract valuable information from an organization without being detected. Preventing these attacks is more about Data Loss Prevention (DLP) rather than resiliency.

3.5 Best Practices in Cyber Security and Resilience

The most comprehensive and definitive sources of guidance on information security practices is found in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-series. NIST has dedicated substantial resources to this important cause, and maintains a breadth of documentation providing best-practice guidance across numerous disciplines within information security.

Recommendations in the NIST documents are based on extensive collaboration with key federal departments such as the Department of Homeland Security (DHS) and the Department of Defense (DoD), their various agencies, and include collaborative findings and guidance from interaction with numerous commercial and non-profit organizations.

The most important NIST documents to be familiar with essentially define the groundwork for all information security practices and processes. Although these documents are written for Federal entities, they are widely regarded as definitive and authoritative standards for all industries and information security practices. NIST maintains and updates these publications to remain current with changes in relevant technology segments, and the documents are generally consistent with, and complementary to other established information security standards:[16]

1. NIST SP 800-39 Managing Information Security Risk[17]
2. NIST SP 800-37 Revision 1 (Jun 2014) Guide for Applying the Risk Management Framework[18]
3. NIST SP 800-53 Security and Privacy Controls[19]

For a local government to benefit from NIST documents, it must read and apply them directly, as well as require that its systems, applications, and solution providers are compliant with them as a matter of policy.

Additional resources—including geographically specific resources—for state, local, tribal, and territorial (SLTT) governments are available on the US-CERT website.[20] These resources focus on the specific and unique needs of SLTT governments, and offer support to identify, protect, detect, and respond to cyber threats.

[16] "About CSRC," Computer Security Resource Center, National Institute of Standards and Technology, https://csrc.nist.gov/about, accessed October 2017.

[17] "Managing Information Security Risk: Organization, Mission, and Information System View," Computer Security Resource Center, National Institute of Standards and Technology, Mach 2011, https://csrc.nist.gov/publications/detail/sp/800-39/final, accessed October 2017.

[18] "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," Computer Security Resource Center, National Institute of Standards and Technology, June 5, 2014, https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final, accessed October 2017.

[19] "NIST Special Publication 800-53," National Vulnerability Database, National Institute of Standards and Technology, https://nvd.nist.gov/800-53, accessed October 2017.

[20] "Resources for State, Local, Tribal, and Territorial (SLTT) Governments," United States Computer Emergency Readiness Team (US-CERT), U.S. Department of Homeland Security, https://www.us-cert.gov/ccubedvp/sltt, accessed November 2017.

4 Case Studies

From small towns to regional consortia to statewide deployments, local and state governments nationwide demonstrate best practices for network pre-planning, implementation, and management. These case studies detail those best practices, as discussed by the staff who have overseen their implementation, assessed their effectiveness, and adjusted their strategies to best address each locality's needs.

4.1 NCRnet

The National Capital Region Interconnection Network, or NCRnet, is a public safety-oriented network that interconnects more than 20 local government jurisdictions in the Washington, D.C., metro area. The network traces its roots to 2004 when the region's CIO group, operating within the structure of the Metropolitan Washington Council of Governments (MWCOG), developed a business case and feasibility study for an infrastructure that would facilitate interoperable public safety data exchange.

Based on that study and additional engineering and strategic planning efforts, the Department of Homeland Security's Urban Areas Security Initiative (UASI) funded the construction of interconnection fiber to link the local governments' existing fiber networks. (The local governments typically had fiber strands available as part of their cable franchise agreements and agreed to dedicate a fiber pair from each of their hub locations for NCRnet.)

The network, which was largely completed by 2011, connects the District of Columbia, all of the surrounding counties in Maryland and Virginia, and most of the autonomous city governments in the metro area. Because those jurisdictions' public safety agencies were already connected to their own respective jurisdictional networks, NCRnet connections extended the physical paths from the local public safety agencies to the partner agencies.

Other participating entities include the Metropolitan Washington Airports Authority (MWAA), which is connected at both Dulles International and Reagan National airports; the Washington Metropolitan Area Transit Authority (WMATA); and several federal partners, such as the U.S. Park Police and FBI's closed-circuit television network.

4.1.1 Setting Goals and Objectives

As NCRnet was conceived and developed, the lessons of 9/11 for interoperability and resilience of voice communications were driving many concerns on the public safety radio side. But the region also foresaw the need for developing similar resilient infrastructure on the network side. These requirements were developed as part of the concept of operations and included the need for the network to be cost-effective, both in terms of capital and maintenance expenses; the network had to be financially sustainable in the long run, given that it would be maintained by the participating jurisdictions.

In addition, to meet the public safety mission, the network needed to be high capacity, high security, and high availability. High availability meant that it needed to be largely independent of commercially switched networks. The concept was a private network that would work exactly when commercial networks would be congested or unavailable, such as during regional events. And, unlike publicly switched networks, NCRnet would be exclusively for public safety and emergency response related traffic.

The network needed to be flexible—able to support any type of application—and scalable, so it could add new partners. It also needed to allow for changes in configuration as needed to meet specific network requirements. And it had to be future-proof—capable of meeting future bandwidth and technological needs without the need for a complete redesign of the network.

4.1.2 Defining and Designing the Critical Infrastructure

4.1.2.1 Defining the Options for Interconnection Builds

At the time NCRnet was conceived, almost all partner jurisdictions had their own fiber institutional networks (I-Nets) provided by the cable companies. To meet the public safety-driven objectives, the project had to determine how best to deploy new interconnection fiber to link the I-Nets. The fiber NCRnet infrastructure would be defined by these new links and by existing jurisdictional fiber segments that would bring the connectivity back to jurisdictional hub sites where NCRnet electronics would be placed. Jurisdictions typically allocated two fiber strands from the hub sites to a meet-me point, from which the project would construct a new link.

NCRnet's planners established two primary design principles for the links between participating jurisdictional sites, as described below.

4.1.2.2 Preference of Dark Fiber Over Lit Services

Dark fiber can be provisioned with any type of service and bandwidth and is only limited by the electronics attached to it; those electronics can be upgraded and replaced as needed without any change to the fiber or the necessity to change a contract with a service provider. Dark fiber is also defined on a site-to-site basis, so there is transparency for the user in terms of the fiber's path and method of deployment. This in turn allows future projects to design routes with path diversity.

By comparison, most carrier-provided lit services are provisioned at a remote carrier hub—and it is difficult, if not impossible, to receive information from the carrier about the service's actual physical path. Thus, with lit services, it is often impossible to understand the risk posed by single points of failure and lack of path diversity. The way lit services are provisioned also makes it difficult to patch together different segments from multiple providers into a seamless network, and further complicates issues of scaling and risk assessment regarding reliability and resilience.

Lit services also introduce unknowns into both service restoration and security incident management. The choice of services is limited to the speeds and protocols that a service provider offers in a given area. Change management often is difficult, lengthy, and time consuming. And because government clients are relatively small customers compared to enterprise clients, they are often last in line when carriers restore services.

4.1.2.3 Building and Owning Fiber Preferred Over Dark Fiber IRU Leases of Existing Provider Strands

There are two main options for procuring dark fiber. A jurisdiction can build its own fiber, or it can procure a long-term lease of someone else's fiber. The latter option most often takes the form of an Irrevocable Right of Use (IRU) and involves a limited number of strands (typically two) out of a backbone bundle of fibers, along with a "lateral" fiber built by the provider to connect the backbone fiber to the client site.

IRUs are a convenient arrangement for local governments because the fiber providers maintain the backbone fiber, while the leased strands are assigned to the locality for its exclusive use. IRUs can be cost-effective alternatives to owning fiber over longer distances, where building on one's own is cost-prohibitive—assuming a provider has existing excess strands for most of the distance required, and is willing to lease.

But because the IRUs operate in an open market where governments have to compete with businesses that often derive direct value from dark fiber—or are able to monetize the fiber—the cost can be very high for governments. A two-strand IRU also means that the government will have to make do with only those two strands.

In contrast, if a jurisdiction installs its own fiber, the incremental costs for adding large number of strands when building fiber is relatively small, making the need for both physical segmentation and connecting future sites along the fiber path much easier and less costly. Further, while IRUs give better risk disclosure and management than lit fiber, owning fiber gives full control over repair, physical path changes, allocating multiple strands for different purposes, and interconnecting with third parties. When maintenance is performed by the IRU provider, it is not always feasible to ensure strong controls in the agreement for restoration, updated engineering drawings for as-built documents, and service levels.

Ultimately, while the NCRnet jurisdictions' cable franchise-provided fiber was satisfactory for the objectives outlined by the stakeholders, it became an issue of contention for cable providers as NCRnet interconnected with more partners and into commercial data centers where some of the public safety applications were hosted.

4.1.2.4 Building the Interconnections, and Defining the Network

While owning fiber was recognized as optimal for public safety purpose, the practical reality in the beginning of the project meant that all early builds used the franchise agreement framework to secure fiber from the cable operators, which is a third approach between owning fiber and leasing it.[21] The new builds had to interconnect with existing fiber that was franchise fiber in the first place, thereby limiting any advantage of the jurisdictions constructing dark fiber on their own.

In addition to meeting almost all the objectives for public safety and being cost-effective, these interconnections were also typically fast to deploy since cable operators could take advantage of existing poles and fiber. The cost and speed of construction were further improved by the cable operators' ability to leverage their extensive infrastructure to minimize the length of the required new builds: A cable operator is often able to build from the nearest splice box rather than a more distant hub facility.

The government procurement process is often a risk factor in projects such as this because construction needs to go through RFPs unless there are existing contract vehicles in place. For franchise fiber installation, the procurement process used the existing franchise agreements instead. Governance was also relatively well defined, since existing agreements made clear who maintains what, and at what cost.

Because the interconnections were grant-funded, using franchise fiber owned by the cable company eliminated a range of other complications, as well. Otherwise, the jurisdictions would have needed to go through a complex asset transfer process—given that there would have been a sponsoring jurisdiction responsible for managing the grant, a procuring jurisdiction, and a receiving jurisdiction.

4.1.3 Assessing and Analyzing the Risk of Franchise Fiber

The NCRnet project assessed the risks involved with franchise fiber and identified a number of areas where risk either had to be mitigated or accepted. This included:

- *Limited fiber count allocated to government:* Franchise agreements often limited the number of fiber strands to six, sometimes a few more. Later, as minimum strand size sheaths available for franchise cable operators increased, the size increased to 12, then 24, and in some cases 48. The initial limitation in strands, however, also limited the ability to use the same segments for other interconnection opportunities with new partners.

[21] Some jurisdictions had a perpetuity clause for the fiber so it would become the jurisdiction's if the agreement terminated without renewal—but in practical terms only the cable company can access and service it, and the cable company retains the right to relocate it as needed.

- *Inconsistent technical specifications for fiber:* Franchise agreements usually referenced technical standards for testing fiber, but these agreements often suffered from inconsistent technical standards for loss budget and power meter, lack of specifications for type and quality of fiber used, and lack of general engineering and safety standards for construction and splicing. NCRnet could not simply adopt a set of uniform standards that could be adopted for all constructions.

- *Restricted use to internal government-only traffic:* Franchise agreements often restricted allowable use of fiber strands to internal government needs, so *inter*-governmental connections were a grey area in many cases.

- *Non-conveyance of fiber:* Since franchise fiber was owned by cable operators or specifically restricted, excess fiber strands could not be shared, swapped, or traded with other regional entities—even if that would have been the most effective approach to building out the network. Other regional networks, including state, university, and WMATA systems had used such approaches to connect sites that would otherwise be costly to reach.

- *Weak service-level agreements:* SLAs for fiber repair were inconsistent and/or not well defined or followed. In most cases, cable operators were cooperative when a fiber break was identified, but because the fiber strands were not part of a fee-for-service arrangement, there was effectively no mechanism to penalize the cable operator for not meeting an SLA. There was no bill against which to apply a credit.

- *Lack of access to cable-provider-owned hubs:* Cable operators were not always cooperative in granting timely access to its hub sites where NCRnet equipment was stored; this created issues when testing had to be conducted and when the jurisdictions needed access for network equipment installation, upgrades, troubleshooting, or repairs.

- *Limited insight to actual fiber paths:* Franchise agreements typically identified the legacy sites to which fiber was built—but little more in terms of identifying fiber location. Actual paths were not disclosed. With new interconnections built under such franchise agreements, paths were sometimes disclosed during engineering walkouts and permit processes, but actual engineering as-built were rarely provided

- *Limited ability to splice/interconnect directly with other fiber providers:* Restrictions on the ability to connect at the nearest splice point meant that jurisdictions had less flexibility and cost efficiency, and further limited options in terms of potential opportunities for interconnection—which were sometimes lost despite close physical proximity between existing fiber plants.

4.1.4 Assessing Other Risks

Risk assessment activities were conducted in monthly meetings by CIOs and CISOs, and on an ongoing basis by the NCRnet team. In addition, as the project sought to address potential weaknesses after all partners were interconnected with at least one link, a formal risk assessment study was undertaken.

4.1.5 Implementing Risk-Management Activities

NCRnet employs multiple strategies to address and mitigate risk. While some are based on the physical infrastructure itself, others focus more on internal policies and actionable procedure to build resiliency and security into every facet of the network.

4.1.5.1 Initial Risk-Mitigation Strategies Adopted by Jurisdictions and NCRnet

The identified risks led to a number of mitigation strategies, including:

- *Documenting fiber paths:* For disclosure of actual paths, NCRnet project engineers would conduct joint walkouts as part of feasibility studies and document the path, or jurisdiction staff would try to reverse-engineer the paths where possible and document in their own systems. The NCRnet project maintained solid documentation of accumulated knowledge regarding paths.

- *Negotiating higher fiber counts:* In many cases, NCRnet could negotiate higher counts than respective franchise agreements technically allowed.

- *Overbuilding:* Some jurisdictions also found opportunities to later overbuild on particular stretches with scarce fiber to make up for the strands they had to allocate to the NCRnet project.

- *Assigning the highest priority for repairs:* Some jurisdictions had formal or informal mechanisms for categorizing links and stretches as priorities. Where feasible, they assigned NCRnet fiber to the highest category.

- *Selecting reliable electronics*: To mitigate against lack of hub site access, NCRnet selected electronics that had proven reliability records to minimize the need for accessing sites for failing electronics.

- *Employing uninterruptible power supplies and out-of-band modems:* Power and remote management meant NCRnet engineers could troubleshoot issues without needing emergency access, such as over weekends or on holidays.

4.1.5.2 Risk-Mitigation Strategies for Jurisdiction-Owned Dark Fiber

While cable franchise agreement fiber strands were initially the go-to vehicle for constructing the interconnection network, the franchise operators increasingly declined to cooperate on building new extensions, and recently have declined to renew such agreements for existing fiber in perpetuity. Coming at a time when fiber is more needed than ever to satisfy jurisdictional data needs, both current and projected, the lack of a cost-effective alternative for fiber growth through the cable operators represents a major risk for the jurisdictions. This has dramatically changed the environment for both jurisdictions and NCRnet. In response, jurisdictions, and NCRnet by extension, have adopted a number of risk-mitigation strategies:

- Many jurisdictions are now building their own fiber.
- Many now have construction procurement vehicles and have added cooperative purchasing riders so neighboring jurisdictions can take advantage of them.
- New extensions by cable providers, when cooperative, are folded into existing networks to provide uniform maintenance governance.
- Those governments building on their own typically install large fiber counts since the cost differential is minor.
- Jurisdictions and NCRnet try to steer builds away from cable hubs to government facilities for better access.
- Some jurisdictions hire ex-cable engineers to reverse-engineer physical routes and generate as-builts into fiber management tools.
- Some jurisdictions negotiated the ability to place remote test units on unused fiber pairs to proactively monitor and repair the fiber.
- Some negotiated the ability to interconnect with other governments and non-commercial partners.
- Some negotiated the ability to repair fiber themselves if the cable provider is unable to meet its SLA for dispatching a repair crew.

4.1.5.3 Adopt Resilient and Secure Physical Design

NCRnet’s current physical design uses resilience as a guiding principle. Because all partners are interconnected, redundancy and resilience must be prioritized where it makes the most sense. To that effect, NCRnet adopted the following design principles:

- *When possible, pursue options for constructing redundant paths.* Prioritization for which jurisdictions to target is done according to criticality. A risk assessment scored all NCRnet sites for power, diverse entry, and other considerations, and higher priority was assigned to jurisdictions that hosted or participated in mission-critical applications such as regional mutual computer-aided dispatch. In addition, higher priority was assigned to "core" jurisdictions that provide mutual aid and technical support for smaller jurisdictions during regional incidents, have more resources to assist in quickly restoring services, and serve more public safety users.

- *When feasible, pursue diverse path entry.* In practice, such strategies are opportunistic to keep costs under control when a jurisdiction or partner constructs new fiber nearby.

- *Create rings where feasible.* Designing such rings at the physical layer allows NCRnet to leverage self-healing electronics that quickly reroute traffic if a site or link goes down.

- *Define more than one point of ingress/egress for site diversity where feasible.* This means not just having more than one site for interconnection, but also connecting firewalls at different sites for entry in and out of the jurisdiction network. Here, too, the prioritization and urgency of such activities is a function of criticality of application use or hosting. In the case of the mutual aid computer-aided dispatch application, all participants in that project are prioritized for finding ways to pursue such strategies.

- *Consolidate NCRnet equipment in one rack to avoid misconfiguration.*

4.1.5.4 Secure and Resilient Networking

In addition to the approaches taken for the physical topology, NCRnet has adopted several principles for resilience and security at the network layer. NCRnet uses Juniper MX80s for core and edge networking. Along with other electronics and policies, this equipment allows NCRnet to:

- *Use MPLS for segmentation.* For example, sensitive biometric applications are segmented into their own VPN for that purpose, insulating those applications and making it easier to provide end-to-end separation all the way into a server inside a jurisdictional network, if policy dictates. Issues affecting this VPN will not affect other traffic and vice-versa.

- *Highly control the process for applications on the network.* All applications on NCRnet are assigned an NCRnet public IP address, require approval prior to deployment on NCRnet, and go through a Change Advisory Board review. This means unauthorized traffic is immediately flagged and can be blocked.

- *Monitor the network*. Intrusion detection system sensors and other advanced security tools are placed at all aggregation points to capture all traffic on NCRnet. To separate the network, reverse proxy is employed at the data center for anything requiring access to the internet.

- *Maintain consistent and standardized peering with all partners and third parties.* This approach makes it easier to troubleshoot, patch, and upgrade; and keeps the skillset required of NCRnet staff manageable. Peering arrangements will differ according to aims. The trick is to try to adopt as much consistency as possible, while understanding that it is impossible to standardize completely. In NCRnet, that means that all peering is accomplished with consistent edge router hardware platform and configurations, [22] or a regular ethernet peering arrangement for specific dedicated traffic (such as radio-over-IP). For non-partner untrusted connections, NCRnet also places a firewall and traffic sensor on its side of the demarcation to block unwanted traffic.

  More importantly, it means documenting the interconnections and ensuring the interconnecting partner is responsible and accountable for its side of the demarcation, even if part of the interconnectivity is provisioned through additional partners or carriers or serve other downstream customers. A standardized high-level demarcation diagram with example peering showing demarcation line, interconnection method, and documentation regarding mutual notification, escalation, and right to shut off connection should also be standard practice.[23]

4.1.5.5 Resilience Built into Operations

NCRnet has developed a resilient operational capability over the years. NCRnet staff operates its own internal network operations center (NOC) using SolarWinds as well as a number of security tools that ensure issues are quickly spotted.

NCRnet originally outsourced the NOC, but the regional nature of network made it impossible for an external vendor to develop business processes that would direct calls or troubleshooting to the correct site and properly coordinate for troubleshooting. In contrast, on-premises staffing in the Fairfax County Government Center (a facility operated by one of the NCRnet jurisdictions) maintains the learned intelligence of all local partner technical teams and interconnections.

[22] In NCRnet's case, a Juniper MX80 with preferred peering using either an 802.1q trunk connection to a dedicated customer edge firewall or other network device for multiuse traffic.

[23] Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) templates are widely available on the internet and are modeled on NIST 800-47, which provide examples of simple MOUs and ISAs. *See:* "Security Guide for Interconnecting Information Technology Systems (SP 800-47)," Computer Security Resource Center, National Institute of Standards and Technology, August 2002, https://csrc.nist.gov/publications/detail/sp/800-47/final, accessed November 2017.

The NOC actively monitors all abnormal traffic and notifies jurisdictions. In addition, it uses Serena as an ITIL-compliant tool for incident, configuration, and change management and a single service desk. In an emergency, NCRnet can also leverage Fairfax's own staff if needed. Pagers and automated phone trees are used for off-hour emergencies going to both contracted and internal Fairfax staff. All change requests are logged in Serena and must go through an architecture review board for review and approval.

4.1.5.6 Resilience as Process

NCRnet's resilience is not simply a function of designing and choosing the correct infrastructure. It is also an ongoing process. There are multiple features that distinguish NCRnet:

- *Applications drive criticality:* Because NCRnet is public safety application-focused, priorities and criticality are based on applications—and which users are affected.
- *Opportunities to harden with redundant sites, links, and electronics are continually sought:* Knowing application and user needs and the existing infrastructure also means looking for opportunities when they present themselves.
- *Metrics and reporting go to the right people:* Metrics on outages and incidents are shared with CIOs as well as CISOs and network managers. Other metrics regarding application use and participation also go to the emergency support community and executive stakeholders. In addition, special reports are often prepared after regional incidents and shared with CIOs and executive stakeholders.
- *Periodic risk assessments are conducted:* Such assessments flag sites and links that are vulnerable due to power, site and access support, link support, or single points of failure. The assessments identify mitigations and cost options, and they prioritize and recommend improvements.

4.1.5.7 Security Integrated Everywhere

NCRnet developed a Security Policy that was adopted by CISOs, CIOs, and CAOs. It was developed using federal frameworks such as FIPS and NIST. Among other things, the security policy provides the basis that allows a proactive approach to security and allows NCRnet staff to monitor all applications across its network, and to hunt down unauthorized traffic.

The CISO committee is a subcommittee to the CIO committee and is responsible for security on NCRnet. Among other functions it:

- Oversees interconnections with third parties;
- Develops or approves firewall policies;

- Facilitates exchange of information on threats, best practices, tools, training opportunities and procurement vehicles; in particular, larger jurisdictions often provide additional resources and information, including training opportunities for smaller jurisdictions;
- Oversees the regional Identity and Access Management System (IAMS) application which allows single sign-on to regional public safety applications with jurisdictional credentials, and helps ensure that only authorized users currently employed or supporting participating governments have appropriate access;
- Receives and reviews monthly security reporting from IAMS and NCRnet; and
- Oversees periodic security audits of NCRnet

4.1.5.8 Address application layer security with hard and soft power

The onboarding of applications on NCRnet is an opportunity to promote and facilitate use for effective emergency response and an opportunity to promote best practices for application managers and users.

This entire process avoids the "Achilles heel" of such projects: staff turnover results in loss of institutional memory needed to troubleshoot and restore functionality. If configuration and design changes for one piece of an application in one jurisdiction break an application, and no current documentation or history can be found, then the application users often do not know whom to contact for information.

Such onboarding can be difficult to manage for the multiple, disparate teams that make up a regional system. Without a facilitator, even a successful effort can end up causing problems later. Managing this aspect can also become part of a resilient and secure infrastructure.

NCRnet needs to capture technical and functional requirements for all applications. A standard form is used, and an assigned NCRnet engineer facilitates collection of all the needed information. The engineer also coordinates application vendor support, jurisdictional network and applications teams, NCRnet operations teams, and others.

All technical and business contacts are captured, and security requirements based on operational needs are identified. This process also allows the operations team to determine appropriate VRF/VPN and methods of routing and configuration. A diagram is then produced which captures a system-of-systems architecture and flows, and required ports. Working with the operations team, IP addressing is then assigned or allocated.

If there are any unusual designs or requirements for a new application or there are deviations from the standard design that merit review, the request is escalated to the CISOs and network managers for further review. Based on feedback, the operations team then develops technical recommendations as needed for modification. During this process, the applications and operations team often guide and recommend best practices for enhancing application resiliency, appropriate ports, encryption, and integration with IAMS. Once this phase has been cleared and green light is given, the teams develop a test plan, capture baseline performance, and include failover testing when appropriate. During onboarding, the application is integrated into the NCRnet operations' monitoring tool.

4.2 Arlington County, VA

Arlington County has operated a County fiber optic network since the late 1990s, when the County negotiated with the cable operator for dark fiber connectivity to approximately 80 government, school, and library locations. The County's Department of Technology Services (AC DTS) and Arlington Public Schools (APS) each acquired electronics and operated two separate networks. Each site has 12 fibers in a star topology to either the County hub at Courthouse Plaza or the APS hub at the Education Center. Originally, the County network focused on IP data and voice, and government applications.

As the needs of the County surpassed the limited number of fibers the cable operator provided, the County utilized limited CWDM technology in some places to mitigate its low fiber count, enabling the County to double or quadruple the capacity of individual fibers. Several years ago, the County saw that this cable operator-provided fiber network would be inadequate to meet the County's future needs—not only in terms of number of strands, and the limited ability to negotiate a solid fiber performance SLA from the cable operator, but also as it anticipated that the cable operator would be unwilling to expand, augment, or properly maintain the network. Additionally, the County recognized its need and desire to have the full flexibility of its own fiber network to support economic development and partnership objectives that were limited under the terms of the franchise agreement.

The County is in the process of completing the construction of ConnectArlington, using County-owned fiber to replace the fiber supplied by the cable operator, and has almost entirely migrated away from any cable operator-owned hub sites or fiber.

4.2.1 Setting Goals and Objectives

The County has stated four goals for its network infrastructure:

1) Operate a network without reliance on outside service providers,

2) Leverage fiber already being constructed for intelligent transportation system networking,

3) Reduce the County's risk of having to pay lease fees or other compensation to the cable operator upon renewal of the cable franchise agreement, and

4) Potentially make county fiber available for lease to the private sector and other economic development applications.

In addition, the County requires maximizing availability, and limiting any adverse business impacts from any events.

4.2.2 Defining and Identifying Critical Infrastructure

The County treats its network as a critical infrastructure, and has designed its network to minimize outages required for patching and equipment upgrades. From a physical design perspective, the County tries to provide both path diversity and diverse entry where feasible, but there is currently no formal delineation of types of facilities requiring additional hardening. Rather, new facility project sites are reviewed opportunistically to scope redundancy into the design and budget plans.

In practice, its data center, hub sites and major aggregation points are treated with higher priority for restoration, but since criticality is a function of business impact, the County uses a ticket system to indicate the priority of a service request, based on assessed business impact. The County prioritizes links and sites associated with public safety applications such as CAD2CAD and 911 center, but also for partner networks with which it participates regionally in mutual aid, such as MWAA.

Recognizing that network resilience and security depends on recognition and buy-in from stakeholders, the County's CISO has assumed a leadership role, not just in the County government, but also towards external stakeholders, County citizens, the business community, and sister jurisdictions to educate stakeholders about the importance of security and resilience.

4.2.3 Assessing and Analyzing Risks

The County has an architecture committee consisting of the network architect, the CISO, and CIO that review all new projects and major changes. Additionally, it runs frequent exercises with the participation of network, applications, and security teams, after which it analyzes risks and impacts. Its strategic location close to Washington D.C., and its many higher education and research facilities, as well as federal civilian and military partners, provide numerous opportunities to assess impacts on partners.

4.2.4 Implementing Risk-Management Activities

The County addresses and mitigates risk through varied strategies. While some are based on the physical infrastructure itself, others focus more on internal policies and actionable procedure to build resiliency and security into every facet of the network.

4.2.4.1 Adopting a Resilient Architecture

At the physical layer, where feasible, the County tries to provide path diversity and redundancy, especially to aggregation points and its data center, and has incorporated review of new facilities that actively looks for opportunities to ensure resilient fiber connectivity into its processes.

The network core is an always-on system consisting of Cisco Nexus Switches, Cisco Catalyst 6500 Series Switches, Cisco ASA Firewalls, Palo Alto Networks Firewalls, Cisco ASR, and ISR Routers. In addition, it has a Distribution Layer consisting of Cisco Catalyst 6500 Series Switches and Cisco ASR Routers which provide LAN services as well as MPLS VRF services. The Access Layer for end-user connectivity at County facilities (e.g., Edge sites) consists of Cisco's 831, 891, 1921, and 2900 Integrated Services Routers, and Cisco Catalyst 2950, 3560, 3750, 4506 Series Switches.

This architecture, along with the abundance of fiber strands, allows the County to provision redundancy and path diversity either with physical route strands or via its MPLS architecture for applications and partners that are mission-critical.

Because of the different missions of its government clients and its economic development initiatives, the County has created separate functional teams for internal and external uses, and physically separates the two networks through different fiber strands.

4.2.4.2 SLAs and Quality Requirements and Design Specifications

Arlington County has both contracted staff and contracts for fiber repair and network service management with defined SLAs, and monitors performance against the SLAs. Ownership and control over its own fiber allows the County speedy access to its conduits and fiber and gives it full control over prioritization of fiber restoration.

In addition to contracts and documents outlining network management services, architecture, and fiber restoration procedures, the County maintains engineering specifications in a separate document.

4.2.4.3 Risk Disclosure

The County uses a vendor checklist and questionnaire for all contracts as a risk management tool. Since the network was specifically built to avoid dependence on external providers, the County controls all aspects of its network, except for a small remaining portion of Comcast I-Net fiber, which the County will eventually stop using.

The County mandates proper documentation of all interconnections with external partner networks, and treats cloud services as such. For such interconnections, it typically pursues a strategy of both mutual notification and prioritizing redundancy on physical and electronic layers to ensure continuity of operations. Interconnection diagrams, escalation trees and mutual notification contacts are usually captured in a document prior to any interconnection with partners. For an example of the County's documentation, see Appendix H.

While the County has contracted after-hours support for incident management, the need for County personnel to provide facility access and technical staff support results in the County's preference to design remote access and redundancy into edge sites, so that incidents can be handled during regular business hours without affecting performance.

4.2.4.4 Change Advisory Board/Security Controls

All changes and interconnections are reviewed and approved by a change advisory board (CAB) process with participation from key stakeholders, CISO and network teams. In addition, the County maintains strict policies for interconnection of partners that control not just inbound, but also approved outbound traffic within its enterprise network.

4.2.4.5 Tools

The County utilizes a NOC and monitoring tools for fiber, network, and cyber security incidents utilizing formalized contracts for staff augmented services. This allows the County to combine the advantages of on-premises control, rapid response, and knowledge management, with vendor provided expertise and formalized expectations and thresholds.

Other cyber security measures used by the County include:

- Endpoint Protection
- Security Information and Incident Management (SIEM)
- Email Server Protection
- Firewalls
- Network Segmentation

4.2.4.6 Emergency Provisions for Restoration

The County defines emergency procedures for restoration. Because contracted staff is on-premise, the County controls how to deploy its resources to respond for most events. Additionally, the County maintains a separate emergency restoration contract for fiber restoration with an outside vendor for its own fiber, and has procedures for handoff and facility access for the remaining Comcast sites and links that will eventually be decommissioned.

4.2.5 Assessing Effectiveness

The County has defined problem management processes and analyzes metrics for security and network issues. Frequent exercises and testing, as well frequent meetings with peer jurisdictions, provide further opportunities to compare notes and isolate gaps that can further improve resilience and security.

4.3 Fairfax County, VA

Fairfax County operates an extensive 430-site fiber network known as the I-Net, that connects the majority of government facilities and schools. Using dark fiber negotiated from the two cable companies in its footprint, and electronics operated by Fairfax County Department of Information Technology (DIT), the network became fully operational in 2006.

The network has a diversely routed backbone that mostly mirrors the Cox commercial cable broadband network backbone. County hub facilities are collocated with the Cox backbone, with the addition of the Fairfax Government Center as a major hub site. The County operates a multiprotocol label switching (MPLS) network with a dense wavelength division multiplexing (DWDM) backbone. The network serves county government and Fairfax County Public Schools (FCPS) sites.

The initial franchise agreement, like many other such agreements in the DC metro area, granted Fairfax County six fiber strands to existing facilities and a cost-plus framework for constructing to additional sites. The objective of this deployment was initially limited to simple cost considerations as use of dark fiber significantly reduced County costs.

The County continuously reassesses whether remote locations served with copper T1 connections should be migrated to the I-Net, as either bandwidth requirements or expansion of the network footprint can affect the cost-benefit calculation. This reassessment includes the projected periods of occupation at leased facilities, to calculate whether the projected break-even period lies within the projected period of facility use and justifies new fiber construction.

The franchise agreement places several restrictions apart from the limited numbers of strands including: limitations for use exclusively to government traffic and facilities, restrictions for accessing or interconnecting at cable company hub sites where fiber paths aggregate, and rights of cable company to service and relocate fiber as it wishes.

Due to the above restrictions, the County is not currently using this infrastructure to connect to private partner networks for economic development purposes, but has instead focused on ensuring the resilience and cost effectiveness of the network for internal purposes. As the fiber communications network increasingly delivers critical enterprise traffic and supports public safety sites and functions, the County has taken numerous steps to improve the resilience and security of its network.

The responsibility for ensuring resilience and security of the network is chiefly with the Department of Technology, and the Chief Information Officer's office and I-Net and Cable Office. These entities work with facilities management and other divisions in the county to anticipate and address security and resilience issues.

4.3.1 Setting Goals and Objectives

The County's primary goal is to provide connectivity to its own facilities for internal data and communications purposes. The I-Net provides better availability, capacity, and continuity of operations than locally available commercial offerings, so the County prefers to deploy I-Net fiber rather than using commercial networks. The County also requires network separation between different facilities, user communities, and data traffic type—in part because of federal regulations regarding use of personal identifying information—and therefore needs to be able to segment the traffic both physically and electronically.

4.3.2 Defining and Identifying Critical Infrastructure

Since the County considers its enterprise computing essential, the entire network is considered critical. However, the County has determined that it needs to provide special hardening to core network sites and police stations to minimize disruption in availability to these sites.

The County has required critical treatment at some new sites, including new police stations, and the McConnell Public Safety and Transportation Operations Center. Future critical sites may include schools that could be designated as shelters, as well as existing community centers that are currently designated as public shelters.

To anticipate and mitigate any need for costly hardening in the future, the County institutes a process where any new potential building projects from facilities management are screened by a technical team. This process assesses alternative sites relative to the cost of adding redundant, path diverse fiber connectivity to those sites, and estimates costs that are then included in the capital building project budget.

4.3.3 Assessing and Analyzing Risks

The County engages in frequent all-hazards exercises in which both voice and data communications are tested against a variety of scenarios. Lessons learned from outages are used to evaluate relative risks and impacts and can inspire changes in physical, network, segmentation, or security controls.

To ensure continual proactive monitoring of the network, the County has implemented its own monitoring at the physical, network, and cybersecurity layers. For after-hours monitoring, the

County has contracted with an external NOC, though its own system usually captures events faster and automatically notifies designated staff, even after-hours. Designated staff receive and respond to outages throughout the day using an automated on-call system.

These monitoring systems provide additional intelligence regarding current and trending risks, and allow the County to adopt mitigation strategies as needed.

While the County has a cooperative relationship with its main cable company—Cox Communications—that provides most of the fiber for its I-Net, the criticality of its infrastructure has led it to adopt a variety of approaches to provide to address its chief risk factors at the physical layer: lack of sufficient information, and proactive intelligence regarding potential issues. The County has hired an experienced OSP engineer that has enabled the County to update its detailed GIS-based database of its current infrastructure, incorporated the need for providing as-built documentation for new builds, and developed cost estimation tools to develop business case assessments of new or redundant links more accurately and rapidly.

The County has an agreement with Cox for fiber testing and quality assurance inspections, and has both in-house staff capabilities and contracting vehicles for outside vendors to perform this function. On spare fiber, the County has installed remote power metering systems at its sites, allowing it to often note potential abnormalities in the fiber bundle before they affect the network.

To obtain a deep base of information from the vendors that supply network electronics, services, or staff, the County developed a vendor questionnaire that assesses security practices and risk-management activities and standards adopted by its vendors. This allows the County to better assess risks when utilizing outside support.

4.3.4 Implementing Risk-Management Activities

The County adopts a comprehensive approach to risk management, employing preventative, ongoing, and reactive strategies to maximize network functionality.

4.3.4.1 Adopting a Resilient Architecture

To ensure continuity of operations and resilience, the County has adopted a physical and network architecture around a modest number of strands in its backbone. The network utilizes a DWDM core with Cisco ASR9006 or ASR9010 equipment, depending on the site. All other I-Net equipment uses MPLS technology, which creates diverse network paths and provides a high degree of flexibility to manage the network. MPLS is a highly versatile protocol, but requires highly trained staff to deploy and operate. Because of its flexibility and ability to segment and manage traffic, it is well suited to a large-scale network of this type, with complex resiliency and security requirements.

The network is configured so that the MPLS layer fully creates the necessary path diversity, even if the diversity created by DWDM fails. The current equipment is the second generation of electronics, and it was installed over a seven-year period at a cost of $14 million.

The network is divided into several discrete virtual routing and forwarding (VRF) segments based on application type. The MPLS-based VRF segmentation enables the County to contain adverse impacts at the cyber level, and scales well with additional sites and users. Current VRFs include public data, electronic payment, mail, voice, SCADA, sewer, HVAC, CCTV, public safety dispatching, criminal records, water authority, and Internet of Things/building automation.

There is also a legacy CWDM32 network for redistribution of the commercial and public, educational and government video content. This network is being replaced by an IP-based approach using the MPLS network.

4.3.4.2 SLAs and Quality Requirements and Design Specifications

The County's agreements with Cox and Comcast include service level agreements (SLA) for fiber repairs. In the event of a major cut, the cable operator is required to repair in eight hours, and to respond within one hour to a call. There is no SLA for the time to perform new site construction.

The County has negotiated updates of testing specifications and engineering standards through its agreement renewals, because requirements have changed from the original agreements. Early versions only included testing at 1310 nm, but that standard become inadequate as the fiber network increasingly had to be able to support higher speeds with more sophisticated electronics. The County therefore developed an engineering specifications document that it maintains and updates as needed. The franchise agreements refer to this document rather than burying technical language within the agreement itself.

This document also allows the County a one-stop source for design and engineering standards regardless of who performs the work (i.e., the cable company, in-house staff, or contracted vendor support). The document details that solid wavelengths should be stable enough to sustain 100Gbps. This provision also requires that any physical cable must have the same core diameter. Given this, the County insists on using the same fiber manufacturer to avoid core mismatch in splices, which would not be able to sustain higher speeds.

The engineering document also outlines how testing should be conducted, the type of connectors, the use of fusion splicing etc., and also requires bi-directional shots for testing. The loss-level connectors should be pre-certified. It also includes standards for insulation and proper grounding. Other provisions included are procedures for wall penetration (fire stopping), and how much excess coil to leave in the ends, which helps with fiber breaks and relocations and avoids unnecessary additional splicing and budget loss, which has proven especially important. It also includes naming conventions for from-to shots so the shots are easily tracked and incorporated into documentation. Finally, it includes quality assurance, from penetration to demarcation, and additional random spot checking.

4.3.4.3 Risk Disclosure

As noted above, the County has adopted a vendor disclosure questionnaire incorporated into the procurement process. In addition, it requires compliance with a set of policies at the user-, vendor service-, and staff augmentation-level that both staff and vendors are required to sign.

4.3.4.4 Configuration Control Board

The County maintains a configuration control board that vets all changes and has both network manager and CISO participation.

4.3.4.5 Tools

At the physical and network layers, the County has developed a dashboard that integrates MapInfo, OSPInSight, and OTDR monitoring systems. That means any operator can quickly see the type and status of circuits at any site. The system monitors fiber, VLAN, video, Metro Ethernet, and TLS, and has recently been upgraded to avoid false positives.

The County has deployed an array of technical controls, providing highly effective balance of cyber security prevention and detection, including:

- Endpoint Protection
- Email Server Protection
- Security Information and Event Management (SIEM)
- Cloud Access Security Broker (CASB)
- Network segmentation
- Firewalls
- Vulnerability Scans

4.3.4.6 Emergency Provisions for Restoration

The County does not have in-house fiber splicing staff, and Cox is responsible for emergency repairs.

In the derecho of 2012, the County's sophisticated system allowed its staff to steer Cox' technicians to priority sites where fibers had to be restored. This enabled the County to direct Cox personnel to critical sites first (e.g., to fire stations before golf courses).

The County also retains supplemental contracts at the network and cyber levels and keeps electronics on hand that its own staff can swap out, rather than wait for a vendor to be dispatched and order any necessary new equipment.

4.3.5 Assessing Effectiveness

The effectiveness of County processes, tools, and mitigation strategies are evaluated on an ongoing basis. Metrics regarding outages and incidents are maintained with the monitoring tools discussed above.

4.4 Holly Springs, NC

The Town of Holly Springs is a suburb in the Research Triangle Region of North Carolina with a growing population of over 25,000. The technically savvy businesses and residents attracted to Holly Springs, which include multi-national firms like the $600 million Novartis flu vaccine manufacturing facility, naturally expect Town staff to deliver government services cost effectively and efficiently using the latest technologies at their disposal. With an ever-increasing dependence on the Town's internal communications networks and IT systems, the need to provide high-availability network connectivity and protect against the ever-increasing number and sophistication of threats to IT security has never been greater for the Town.

Under the leadership of Jeff Wilson, Director of the Town's Department of Information Technology, the Town has met these challenges and growing demands head-on. In recent years, the Town has made great strides towards facilitating ubiquitous and robust network and broadband connectivity and IT services, both internally and among the Town's businesses and residents, while maintaining strong controls over security and the ability to deliver services reliably.

In 2013, Holly Springs analyzed the business case for constructing its own fiber optic network to interconnect its eight primary facilities, with an eye towards future expansion and a broader range of connectivity needs. This analysis concluded that the Town would pay less overall compared to leased communications services by building and operating its own fiber network, while enabling the Town to architect a network having drastically enhanced resiliency and capacity compared to more expensive leased services.

The Town now operates and maintains its own fiber network, which spans nearly twice as many route miles as originally planned. The network provides extensive physical path diversity for connections between critical Town facilities, as well as redundant connections to outside networks and service providers. Backbone connectivity for public Wi-Fi, water and sewer utility systems, and traffic signal controllers are a few of the expanded roles of the Town's network today.

The forward-looking design of the network had a role in attracting Ting Internet, a relatively new entrant to the commercial fiber-to-the-premises (FTTP) market. The network provides an ongoing revenue stream to the Town in the form of dark fiber leases to Ting, while helping to enable increased competition and the delivery of advanced broadband service offerings to the Town's businesses and residents.

As a case study in achieving network resiliency, the Town of Holly Springs offers many examples of employing best practices at an appropriate scale, from the planning to the operational phases of its IT infrastructure.

4.4.1 Setting Goals and Objectives

From its initial planning phase, the Town's primary goal for its fiber network infrastructure was to reduce or eliminate dependence on commercial providers to support critical IT services, thereby enabling the Town to:

- Mitigate the risk that its future needs will exceed the capacity of services that it can afford;
- Control aspects of the network design and operations that directly impact network resiliency; and
- Make spare fiber and conduit capacity available for lease by the private sector to support economic development initiatives and the delivery of advanced services to its residents and businesses at more competitive rates.

4.4.2 Defining and Identifying Critical Infrastructure

The Town considers its network to be critical infrastructure, given the wide range of IT services and communications applications it supports–enabling the capabilities necessary for daily administrative functions of local government, as well as the delivery of public safety services. The many sources of risk to the network, whether posed by manmade or natural threats, represent potential impacts ranging from financial loss to the loss of human life.

With more of the Town's IT systems moving to cloud-based providers, including Microsoft Office 365 for e-mail and other unified communications services, reliable internet connectivity has also become more critical than ever.

The Town's Enterprise Resource Planning (ERP), public safety dispatch, and police records systems are also among the most critical IT resources, for which no degree of outage is deemed acceptable. The ERP system is necessary to write checks to support restoration efforts following a disaster situation, and is also used to track safety inspections. A devastating EF3 tornado that passed through Holly Springs in 2011, nearly destroying one of the Town's fire stations, demonstrated the criticality of these systems in the aftermath of a disaster, as well as illustrating one of many potential threats to the Town's communications infrastructure.

4.4.3 Assessing and Analyzing Risks

Assessing the potential impact of threats to data security and the availability of communications systems is a key component of developing the business case for measures that may be needed to enhance IT security and network resiliency. Understanding risks to IT infrastructure is paramount in the decision-making processes involving financial expenditures for IT systems and infrastructure upgrades, as well as setting IT-related policies that can impact the manner in which government business is conducted. Whether employing network configurations that restrict access or setting policies that require staff to use strong passwords for accessing IT resources, the balance between functionality and efficiency versus security requires leadership to be informed of the potential impact of acting, or not.

Holly Springs' IT Department approaches these trade-offs by continuously assessing risk and making recommendations to Town leadership to mitigate these risks when deemed necessary. The Town's IT Department is guided in part by the requirement to maintain compliance with the FBI's Criminal Justice Information Services (CJIS) polices, which are required for access to important criminal justice databases by the Town's Police Department. Having several departments that accept credit card payments through systems connected to the Town's network, compliance with Payment Card Industry Data Security Standard (PCI DSS) sets additional criteria for IT security assessments.

The Town's network security is enhanced by adherence to these standards on a network-wide basis. Indeed, determining that it was less expensive to employ the required technical measures and enforce IT security policies networkwide to achieve CJIS and PCI compliance, compared to physically segmenting the Police Department network, was part of the analysis that has led to current policy.

Holly Springs demonstrates that a key role of IT staff should be to make a sound business case to their leadership for IT security controls and measures required to improve network resiliency, typically requiring a combination of salesmanship with well-reasoned threat and impact analyses. Aligning analysis with applicable federal standards, in particular those pertinent to local law enforcement (e.g., CJIS policies), can provide local governments with attainable standards that can be applied to the entire network.

4.4.4 Implementing Risk-Management Activities

The Town addresses and mitigates risk through varied strategies. While some are based on the physical infrastructure itself, others focus more on internal policies and actionable procedure to build resiliency and security into every facet of the network.

4.4.4.1 Adopting a Resilient Architecture

The Town's network has been designed to minimize outages at many layers. The architecture incorporates physically diverse fiber paths in the form of backbone fiber rings that pass by nearly all key sites. These rings are optimized to maximize path diversity for the Town's two core datacenter sites, with diverse entry points into each of these.

The network utilizes redundant network electronics to take full advantage of this physical fiber diversity, with nearly all sites connected over redundant electronics links and some degree of physical path diversity.

Redundant datacenters enable real-time mirroring of data over the Town's Storage Area Network (SAN), with similar levels of redundancy of electrical power systems within each datacenter. Datacenter facilities and other larger network user facilities are planned for A+B electrical power configurations, with one side tied to electrical generator power and both connected to uninterruptible power supplies (UPS).

Given the criticality of internet connectivity to the Town's external applications and service providers, the Town's fiber was architected to extend via two physically diverse paths to tie points with NCREN, the statewide research and education network operated by the non-profit MCNC, which in turn enables the Town to connect to dozens of upstream Internet Service Providers.

4.4.4.2 Standards and Policies

Holly Springs has implemented formal IT policies and controls to fortify IT security, including a "Policy on Information Technology" that defines minimum standards for maintaining and using the Town's IT resources. The Policy specifies requirements for IT security training for all staff, defines acceptable uses of the Town's IT resources, restricts usage of personal devices to access Town IT resources, and defines the role of the IT Department in enforcing and approving the usage and modification of IT resources. The IT Policy also references other polices that detail acceptable usage of user accounts and minimum password requirements.

Compliance with the Town's IT Policy is mandatory. IT policies are developed entirely by the IT Department, and approved by the Town Manager. Town leadership does not require IT policies to be vetted by other Town departments. While input from stakeholders is an intrinsic part of the IT Department's approach to defining objectives, analyzing risks, and developing technical solutions based on business case, the Town's approach to developing IT security policy reflects an understanding that it cannot be a democratic process.

The Holly Springs IT Department is seen among Town staff as a responsive provider and enabler of important technology, but the IT Policy helps ensure that a relatively small IT staff can achieve large benefits for the Town. Policies should allow IT Departments to capture cost saving opportunities through interdepartmental collaboration, particularly in relation to capital projects, and by observing internal standards intended to maximize economies of scale with all IT purchases.

Holly Springs' IT Policy requires that all technology purchases and planning be approved by the IT Department. As such, the IT Department was involved in the early phases of planning for a new Law Enforcement Center. IT staff were able to incorporate robust datacenter capabilities into the facility design, and included the planned location for the new facility into the initial design of its fiber network. Once constructed, this facility was able to be activated as a critical datacenter for the Town, with significant cost savings for robust network resiliency features achieved through this forward-looking and timely input into the designs for both the facility and the fiber network.

4.4.4.3 Tools for IT Security and Resiliency

As a relatively small municipality, Holly Springs provides many examples of doing more with less, creating innovative partnerships, and prioritizing expenditures on longer lasting infrastructure offering higher net positive impact, like its fiber optic network.

The Town utilizes internal tools to track network status and utilization trends. All network devices are actively monitored using relatively low-cost network management tools, including PRTG Network Monitor, enabling the IT Staff to view customized dashboards of device status, track network utilization trends, and receive automated alerts when customizable thresholds are exceeded.

Physical security of IT systems is a key component of the Town's overall toolkit. Only IT staff have physical access to datacenters and other locations containing IT systems, with access controls managed and monitored through electronic lock systems and video surveillance.

Since alerting functionality of internal monitoring tools may not be effective if a network outage impacts internet connectivity and/or the core network systems, the Town depends on external monitoring from the Network Operations Center operated by the City of Wilson, North Carolina. Wilson functions as an important backup to Town staff, as well as out-of-band management capabilities that help ensure problems are detected quickly.

Avoiding fiber cuts is one of the most effective approaches to enhancing network resiliency at the physical layer, which was considered by the Town from the planning stages to the development of as-built documentation for its fiber network. Shallow placement of communications conduit containing the Town's fiber was avoided during the construction, but more importantly, the precise horizontal location and depth was recorded and captured within the Town's GIS databases.

Through an effective internal partnership with the Town's Public Works Department, the Town fiber can be quickly and accurately located in accordance with the State's underground damage prevention laws alongside other Town utility infrastructure. As a result, the financial burden of fiber maintenance is relatively low, while enabling the Town to maintain tight controls over this critical function.

4.4.4.4 Emergency Provisions for Restoration

Town IT staff have made modest investments in fiber splicing equipment and related materials to effect small repairs to the fiber network's physical plant when needed, and routinely perform splicing configuration changes. Additionally, the City of Wilson, which has larger fiber repair capabilities to support its own citywide FTTP network, provides on-demand support to Holly Springs on a best effort basis. By monitoring the core network, Wilson's NOC is able to proactively respond to issues. This partnership has proven effective in avoiding outages of the backbone network, and rapidly resolving outages of non-diverse paths when they occur.

The Town has an informal partnership with a neighboring jurisdiction, the Town of Apex, for maintaining spare materials for fiber optic restoration. Through a recently established fiber connection to Apex, the Town intends to expand this partnership to include offsite data storage replication for disaster recovery purposes.

The Town maintains maintenance contracts with rapid replacement provisions for its most critical, core network equipment. Spare equipment is kept on hand for replacement by Town staff for all others, which can be deployed almost immediately in the event of an outage impacting a given site. Since the Town does not maintain IT staffing on a 24x7-basis, the Town has a contract with a Raleigh-based IT contractor to provide on-call engineering support, when required. The Town maintains detailed and accurate documentation of its network electronics architecture and configurations to ensure that restoration efforts can be effected by Town staff or contractors.

4.5 KentuckyWired Network

The Commonwealth of Kentucky began planning a $270 million statewide, multipurpose, public safety-grade fiber optic network in 2013. The Next Generation Kentucky Information Network (NG-KIN) project (later renamed KentuckyWired) started as an initiative of former Governor Steve Beshear to address serious problems with the quality and availability of basic communications and broadband throughout the state. It is the most ambitious network of its kind, designed to eventually connect 1,026 government facilities, schools, and libraries; reach all 120 counties in a rugged, spread-out state; and become the core of Kentucky's mission-critical communications systems. Construction is currently underway with completion scheduled for 2022.

From the outset, the Commonwealth centered its needs assessment and planning efforts around technical, policy, and financial decisions. This process determined the extent and character of users' needs, engaged the stakeholders, and in the end delivered accurate cost estimates and risk assessments. These in turn enabled the Commonwealth to consider and evaluate a wide range of alternatives—technical, business model, operational model, and governance.

Because the existing networks in many parts of the state are primitive and limited, KentuckyWired could, in many ways, be designed as state-of-the-art from the ground up, with less incorporation of legacy infrastructure than if planners needed to leverage existing investments.

Indeed, the quality of broadband in Kentucky generally drops off quickly outside the two major metropolitan areas of Louisville and Lexington, and suburban Cincinnati. Some small islands of the state are served by local telephone cooperatives that deliver high-quality services such as fiber-to-the-premises—but even these areas are handicapped by limited and costly connections to the internet, backbone networks, and data centers.

In many places in rural Kentucky, the only communications infrastructure is the legacy telephone system, which has had only incremental improvements over many years; in terms of broadband, "dial up" or 1.5 Mbps (T1 or low-speed DSL connectivity) is often the norm.

As a result, many of Kentucky's public safety users and other public institutions are unable to acquire high-speed services. They also have to pay several times the cost of comparable services in metro areas.

In addition, these users suffer frequent outages—losing connectivity especially during floods or storms. And because wireline connectivity is fundamental to connecting wireless systems, the limits of the wired networks in Kentucky also correspond to patchy cellular service—and outages in the mobile broadband services used by first responders and government agencies.

After reviewing a range of operational options, including construction and operation of the network by the Commonwealth, partnerships with service providers, and different public–private partnership approaches, the Commonwealth opted to pursue a concessionaire model, similar to toll-road and other infrastructure public–private partnerships in which a partner would share the project's capital and operational risks.

Under this model, the Commonwealth would establish the terms for an entity to create and operate the network, monetize it, and share the cost with the Commonwealth. This concessionaire would need to be responsive to the needs of the Commonwealth and its critical services, and would need to work under a contract that guaranteed those needs would be met

The Commonwealth awarded the contract to a consortium led by Macquarie Capital. Essentially the consortium was tasked with building and managing the network. In return, it would be paid a monthly "availability payment" by the Commonwealth (which the Commonwealth would pay in a similar manner to the service fees it pays to AT&T and other telecommunications providers). After a 30-year contract period, the system would be turned over to the Commonwealth.

The contract includes specific technical parameters described above and specified terms for operations. These include a service-level agreement (SLA) that guarantees packet delivery quality (e.g., latency, jitter, loss), speeds, and uptime, as well as requirements for moves, adds, and changes of sites and changes of services at sites. The SLA also includes regular reporting of network health and trends.

The SLA provides different levels of performance based on the designated criticality of the site. Furthermore, the SLA has different requirements for faults due to the operation of the electronics than for those related to fiber. In the event a problem is caused by a fiber cut, the SLA dictates a time to respond to the cut in the field, but does not specify a repair time, given that the repair time might depend on other utility restoration and other factors beyond the control of the contractor.

The agreement also specifies the number of equipment depot locations that the concessionaire must maintain in Kentucky. The concept was to create a framework where there were (in most cases) sufficient resources to address faults, without quantifying the repair time.

4.5.1 Setting Goals and Objectives

The Commonwealth envisioned a network with physical plant designed to last for decades, driving critical services as well as economic development. KentuckyWired would address the existing communications bottlenecks by building hundreds of miles of backbone fiber and would bring resilient network connectivity within range. Large anchors such as the state's universities and the Kentucky Community and Technical College System locations would host secure and resilient hub locations, and a mixture of local governments and for-profit and non-profit network service providers would build the last mile to interconnect individual homes and businesses.

The Commonwealth pursued a structured approach to implementation that started with a detailed planning process and the identification of costs and risks. The planning process was completed over a six-month period.

The process required intensive collaboration among the project leadership and technical stakeholders. The planning document that emerged from this process accomplished the following:

- Created a prioritized inventory of sites and users.
- Inventoried and assessed both current network services and those needed in the future. The current services include a State-run digital microwave system, copper and fiber

MPLS services provided by the incumbent telephone providers, cable companies, and a few independent fiber companies. Some higher educational institutions were connected through leased fiber.

- Identified applications such as voice and internet that have a likely future need for cloud services—and that were constrained by reliability, speed, and the cost of current services.
- Reviewed network performance—and identified widely varying reliability. A majority of the sites to be connected were on copper networks, so expansion to speeds above 10 Mbps would require the costly and time-consuming installation of fiber.

4.5.2 Establishing Economic Feasibility

It is critical to have a conservative approach when developing business models for building and operating large-scale systems such as fiber networks. Costs should take into account the project's risks by developing a reasonable base model with the likely cost and timeline. It is also important to conduct a sensitivity analysis, in which the model includes the effect of increases in various costs and delays on the project.

KentuckyWired's model included the cost of construction, avenues for financing (and the corresponding costs and risks for each), projections of revenue that might be gained by offsetting existing costs and offering new services, and the operating costs of the network.

4.5.3 Defining and Identifying Critical Infrastructure

The Commonwealth developed a target list including 9-1-1 public safety answering points (PSAP) and dispatching locations, State police stations, data centers, land mobile radio locations, Transportation Cabinet (KYTC) locations, universities, and school systems. Some of the non-public-safety locations were chosen because they were designated as dual-use locations in case of emergencies—for example, schools that would act as emergency shelters.

4.5.4 Assessing and Analyzing Risks

Based on the needs identified, the planning team developed a matrix of technical requirements to attain the required performance and network availability. This matrix included the following factors:

Physical access: Even where facilities would be shared, the Commonwealth required the ability to control site access (physical and electronic), active intrusion detection and alarming systems, and video surveillance. Requirements included logging of access to spaces containing network equipment, proper vetting of personnel, and escorting all visitors.

Backbone redundancy: The network needed path protection switching, load balancing, and geographically diverse paths so that the network could continue to operate while broken fiber was being restored. There would be dual fiber paths from the outside fiber plant into hub buildings, to the fiber termination panel.

Electric power resiliency: This was one of the key factors in outages in the state's existing networks. A fully fiber optic network only requires power at the user sites, not in the outside plant, and would thus reduce outages relative to a copper or cable broadband network. All locations would be configured with uninterruptible power supply (UPS) systems—backup batteries that would keep the network electronics operating for hours in the event of failure and reduce the impact of power spikes on network components. Key locations such as network hubs would require backup power generation to sustain operations over longer periods; in addition to the generators, these sites would require sufficient fuel on hand, and fuel service contracts with sufficient guarantees and storage and delivery resources.

Climate control resiliency: Data center and network closet locations would need to have HVAC systems to maintain environments within the equipment's required operating range. (Even in normal circumstances, equipment heat dissipation can overheat the electronics.) In key facilities, HVAC systems would need to be redundant. In small facilities, it might be possible to consider using outdoor-rated hardened network equipment.

Network electronics resiliency: Key hub sites (with diverse physical fiber routes) required diverse routers, firewalls, and optics.

Site access for network support: In terms of operations, there would be a need for both physical access by support personnel and out-of-band remote management (external wireless or telephone). The majority of faults would be resolved remotely, or with assistance of authorized "remote hands" at the site. Commonwealth network staff would need 24x7 access even if a hub facility were closed.

4.5.5 Conducting a System-Level Assessment

Central to the analysis were detailed discussions with pole owners and right-of-way owners—power companies, telephone companies, the Kentucky Transportation Cabinet (KYTC, the Commonwealth's Department of Transportation), and local governments—to determine right-of-way rules and permitting processes, and the availability of access and space.

From a cost standpoint, KentuckyWired's planners had a significant need to use aerial utility poles. Though there are many functional benefits to building underground, doing so everywhere would drive the construction cost to unacceptable levels. Underground construction also would not be feasible in some of Kentucky's rocky, mountainous areas.

Planners determined that it would be critical to perform a field survey of potential routes, and to have discussions with local contractors experienced in fiber construction to determine pricing and construction risks.

The field survey was a high-level drive-through for purposes of analyzing the condition and capacity of utility poles and the state of the underground rights-of-way. The survey comprised approximately one-quarter of the likely routes and was representative of likely conditions.

The survey identified potential challenges, including that many of the poles traverse private property far from roads. In addition, the survey determined that tree trimming would be a significant issue, and that there would be a significant need to move existing utilities, potentially on as many as 60 percent of poles.

Furthermore, there are dozens of separate pole owners across the state with different terms and requirements, and the Commonwealth would have needed to budget the time and resources to reach multiple agreements, as well as to find creative ways to assist the pole owners with staffing the permitting process for such a large project.

From a scheduling and budgeting standpoint, then the challenge of obtaining access to and using utility poles became the most impactful item for KentuckyWired's planning—requiring two to three years of additional negotiation and work in some parts of the state.

4.5.6 Implementing Risk-Management Activities

The KentuckyWired technical architecture was designed with the ability to serve the most mission-critical users, including public safety, and to cost-effectively serve other users at a range of reliability and survivability levels. To achieve this goal, the network was designed as five separate rings covering different parts of the state and interconnecting 11 or more hub sites (DWDM) and 16 secondary hubs (Ethernet aggregation sites). Lateral routes would extend from the ring, and individual sites would connect to either a ring or a lateral, depending on their location or criticality.

Figure 7 shows the KentuckyWired network with sites identified by the monthly recurring costs those sites were paying commercial carriers for services. These costs are rough proxies for site scale and criticality. The high-value sites mostly are on the KentuckyWired backbone routes or near the fiber rings' intersection points.

Figure 7: KentuckyWired High-Level Statewide Routing

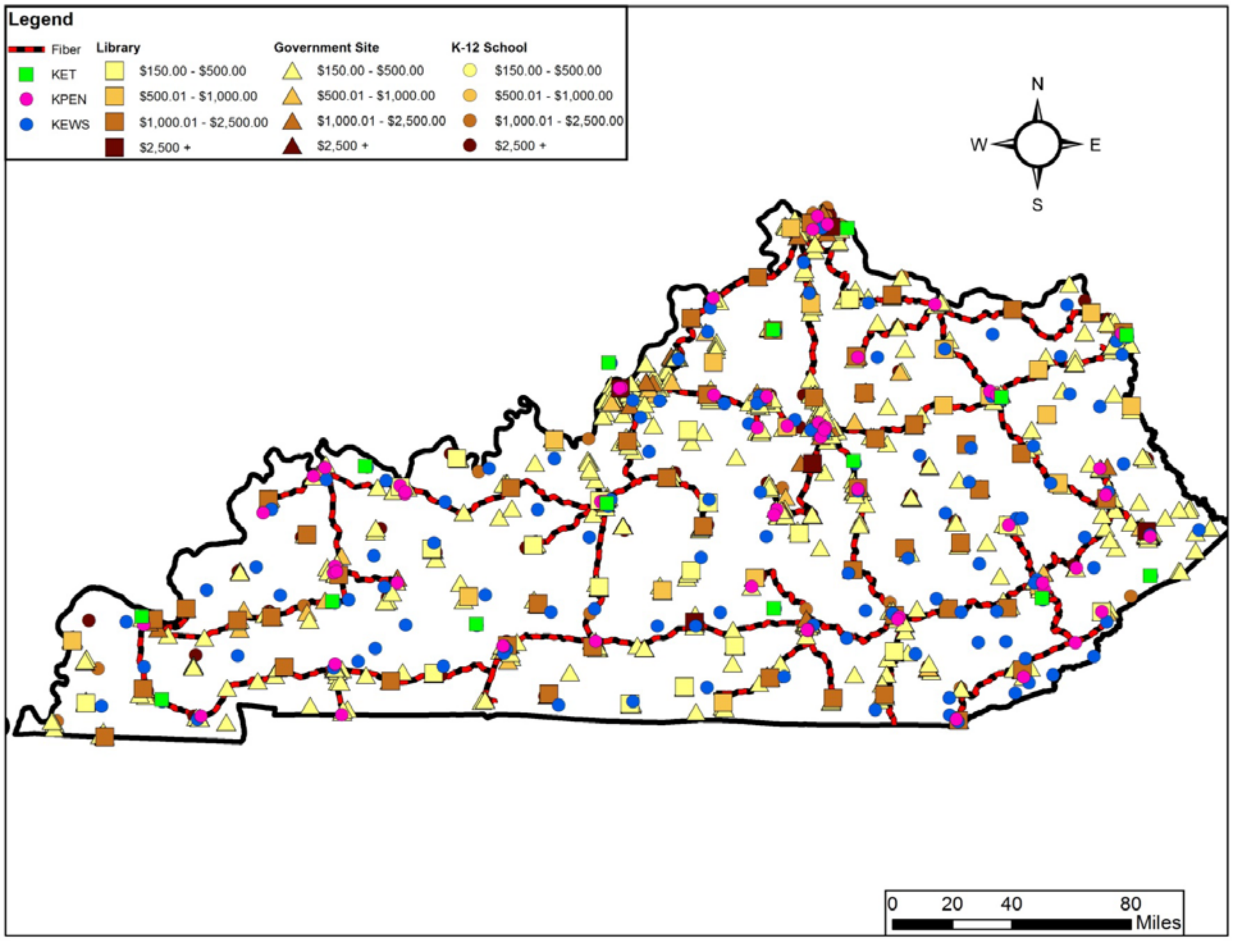
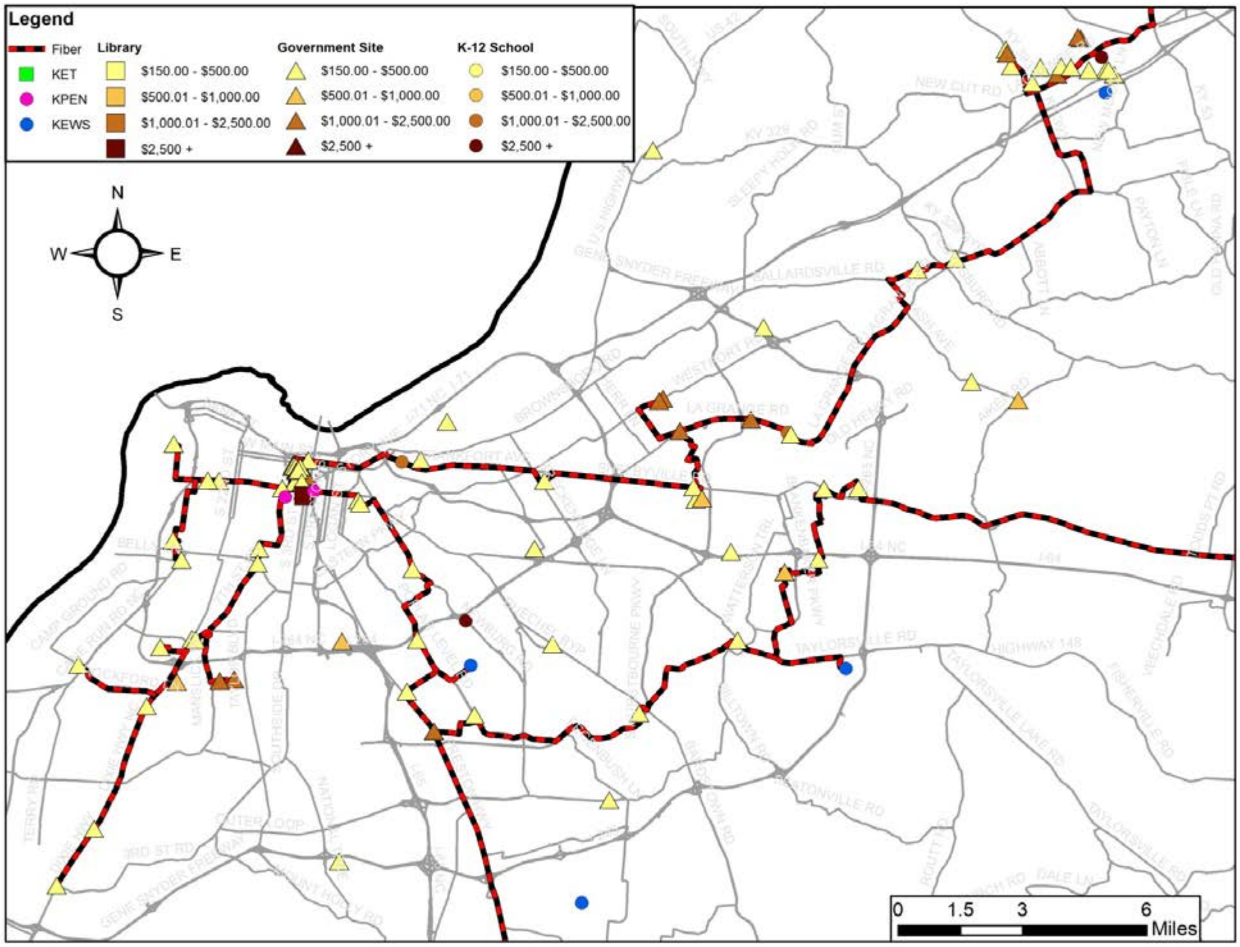


Figure 8 provides a close-in view of the network, focused on metropolitan Louisville.

Figure 8: Louisville-Area Fiber Routing



The network was designed with "lit" and "dark" fiber components. KentuckyWired will operate Ethernet transport services and internet services for public safety and other users over the lit network, and will offer spare fiber to entities such as local governments and for-profit and non-profit service providers over the dark, wholesale component. While the lit services are clearly critical for public safety and other key users, the wholesale side is also important. It will enable services to Kentucky residents and businesses—and will provide revenues to offset the network costs.

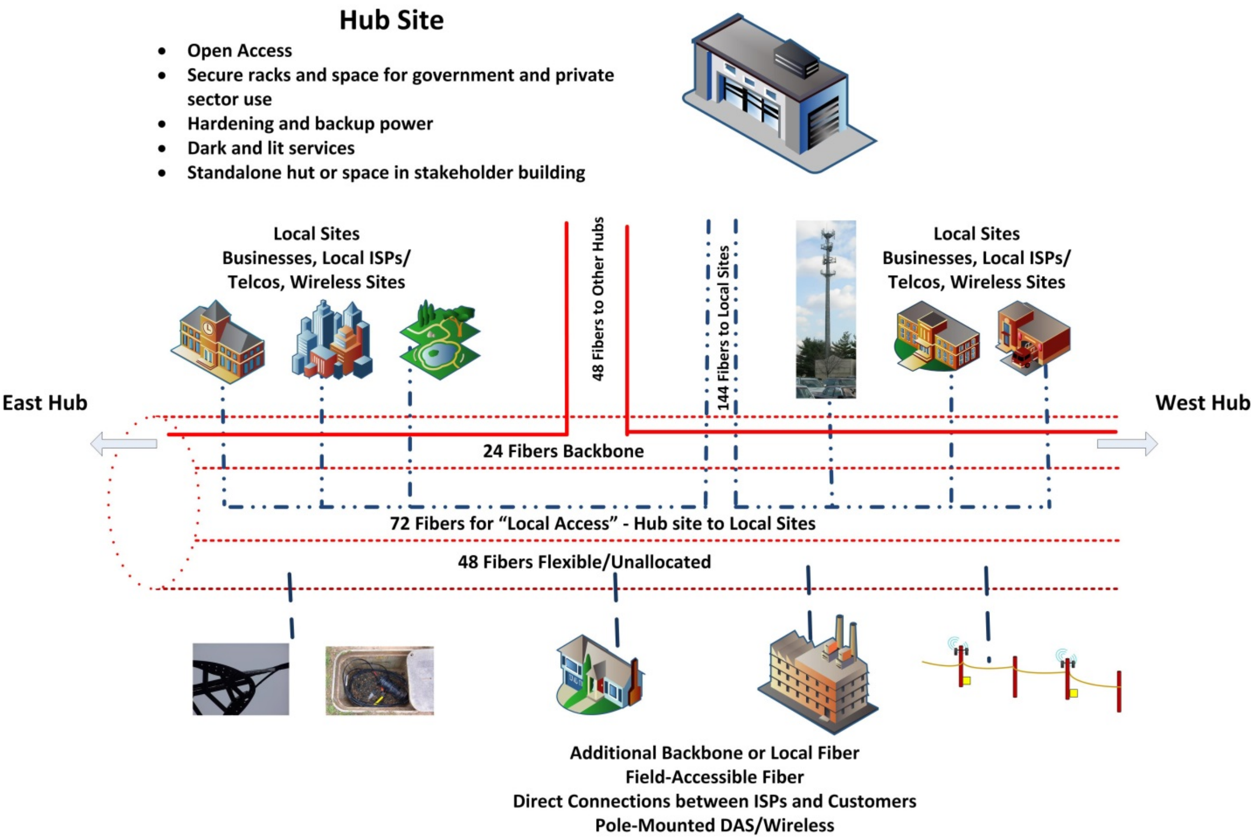
4.5.6.1 Physical Layer

The physical network comprises more than 2,300 miles of fiber ranging from 288-count in the main backbone routes to 24-count to each individual site. It was designed as approximately 75 percent aerial and 25 percent underground. Where it is underground, the fiber will be in two 2-inch conduits, protecting the fiber and providing spare capacity for future use or repairs.

The construction engineering specified G.652.D fiber, due to its ability to deliver high speeds over long distances. Since the fiber is the longest-life component of the network, it was important for KentuckyWired's planners to future-proof it. G.652.D has thousands of times the physical capacity needed today and offers plenty of room to grow.

Figure 9 provides a schematic of fiber allocation in a 144-count backbone route, with separate allocations for backbone, local access, use by public safety and other government facilities, and allocation to service providers for residential and business use. The large fiber count provides the capability to entirely separate commercial users and networks from the public safety/government network and place them on entirely separate fibers, fiber termination panels, and electronics—enabling them to have their own environment within the hubs and entirely safeguard the network. Hub sites are designed according to the standards described above and detailed in Appendix G.

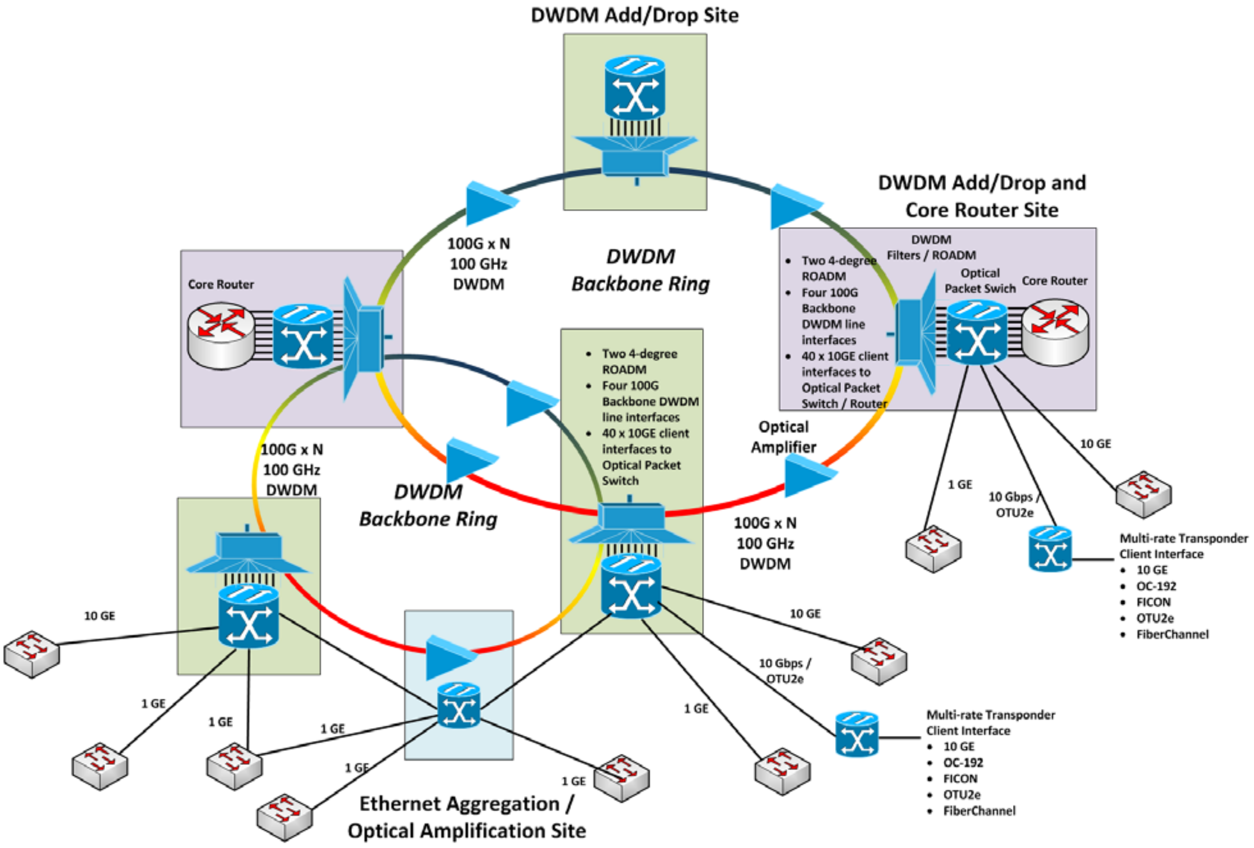
Figure 9: Backbone Fiber Use Schematic


Hub Site
Open Access
Secure racks and space for government and private sector use
Hardening and backup power
Dark and lit services
Standalone hut or space in stakeholder building
Local Sites
Businesses, Local ISPs/
Telcos, Wireless Sites
48 Fibers to Other Hubs
144 Fibers to Local Sites
Local Sites
Businesses, Local ISPs/
Telcos, Wireless Sites
East Hub
West Hub
24 Fibers Backbone
72 Fibers for "Local Access" - Hub site to Local Sites
48 Fibers Flexible/Unallocated
Additional Backbone or Local Fiber
Field-Accessible Fiber
Direct Connections between ISPs and Customers
Pole-Mounted DAS/Wireless

4.5.6.2 Electronics Layer

Because the primary users of the "lit" network are public safety and other government entities, these users drove the functional capabilities of the network. Figure 10 illustrates the logical design.

Figure 10: Network Electronics Logical Design



The network would provide multiple layers of electronics designed to deliver reliability, capacity and security.

The fundamental backbone electronics technology is DWDM (Section 3.4.2.1.4), which provides the capability of multiple 100 Gbps rings and the ability to add and drop individual 10 Gbps connections. The connections simultaneously travel over diverse paths, so in the event of a fiber cut or optics failure, the second path continues to operate uninterrupted. The technology is scalable to add multiple 100 Gbps rings for future capacity. The technology also provides entirely segmented communications, so even in a network where multiple users share the electronics, there can be segmentation—for example, between public safety and the educational users.

Individual sites would connect over Ethernet protocol using either 1 Gbps or 10 Gbps interfaces. The design calls for Layer 2 Metro Ethernet services and enables the separate users to operate point-to-point or point-to-multipoint services, establish connections over diverse paths, and guarantee service levels and capacity. The network design supports MPLS protocols, which support these functions and also enable the setup of networks-within-networks—another layer of security and separation. Again, this can keep sensitive uses and sites separate from others.

Although MPLS creates many possibilities in configuring and operating the network, it and other advanced protocols require well-trained personnel, both in integration and ongoing operations. Therefore, staffing—either of full-time Commonwealth personnel or contractors—became a key part of the budget—and finding and retaining the staff became an area of risk.

Operating an MPLS network of this scale requires a full-time network manager who has familiarity with all the protocols in use (DWDM, MPLS, IP networking). Because this is a supervisory role, the person should be an in-house employee. This person ideally would have many years of experience with the specific protocols or equipment in use—but, if necessary, could be a person with years of general technical network experience and management capability, with the experts in the specific technologies reporting to the network engineer. These experts could be in-house staff or, if necessary, contracted staff.

5 Conclusion and Recommendations

Given the high risk and the high stakes, it is critical that state and local governments plan and implement best practices for resiliency and security and harden infrastructure appropriately. While you cannot anticipate all circumstances or afford to harden everything, it is possible to take many of the steps recommended in this report and also seek further assistance and keep informed as threats and risks, but also solutions, continue to evolve:

- **Ensure that your strategic planning process takes into account resiliency and security.** Having resiliency and security principles in the planning process and planning documents reminds decisionmakers and planners that initiatives need to demonstrate how they are resilient and secure, and make it automatic to ask the right questions when evaluating an initiative.

- **Build segmentation and resiliency into infrastructure.** The examples in the report demonstrate that there are appropriate and cost-effective ways to segment networks, prioritize key areas, create redundancy, and avoid errors in building and placing infrastructure.

- **Make decisions based on lifetime costs.** When considering or evaluating an initiative, it is critical to consider not only the up-front capital cost, but also the ongoing costs such as operations, hardware and software upgrades, training, and staff. Planners also need to include the replacement cost and consider that the different components have different lifetimes—with electronics typically becoming obsolete sooner than fiber optic cables and conduit, and therefore multiple generations of software and electronics being necessary over the lifetime of the physical infrastructure.

- **Ensure you hire and train the appropriate staff.** If possible, hire staff who have significant experience with similar infrastructure, such as those who previously worked in engineering and construction locally with telecommunications operators or utilities, to offer vital "real world" experience. You can improve the quality of staff by undertaking an initiative regionally, so that there is larger scale and therefore more available funding. Often, it is necessary to outsource the most specialized functions to remote network operations centers and contractors or select a cloud-based approach to a function.

  In an operational network, even one that is government-owned and led, the staffing is usually a mixture of contractors and in-house staff, with the balance between the two depending on a specific analysis of the long-term cost of either approach for each position. The analysis needs to take into account: 1) the fully loaded cost for each position, including training and any requirements for minimum staff contract term, 2) the cost of obtaining the same service from a contractor, either in the form of staffing or in services (such as outsourcing a network operations center), and 3) potential synergies with other government roles—such as a customer care position that can also answer 311 information calls or a roads or utilities employee who can handle outside cable plant.

Finally, workforce training programs should include training in resilience and information security, both as a career track but also as an element alongside other technical training.

- **Keep the information security function separate from IT.** Consider that information security is in many ways an auditing function and therefore it works best when it can independently oversee the IT functions of a city or state and provide external guidance.
- **Train for emergencies.** Both internally in department and in the government and with the surrounding region. Exercises can take place as tabletops or in outdoor settings. It should involve the different support functions that will be involved—not just the responders but transportation, public works, and the utilities.
- **Work regionally.** Develop formal or informal consortia for information sharing, joint procurement, best practices, joint exercises and training. The NCR consortium evolved from discussions over brown bag lunches among the CIOs of the Metropolitan Washington Council of Governments (MWCOG). The KentuckyWired network evolved based on leadership and input from its governance group including higher education, public schools, public safety, the Appalachian Regional Commission and local government stakeholders. In the Portland, Oregon area, the public fiber network operators created the Cooperative Telecommunications Infrastructure Consortium (CTIC) to work together and share and trade resources.

There are several ways that DHS and other entities that fund and have a role in guiding state and local government initiatives and those that have a role in regulating them can work toward resiliency and security.

One way is to link funding initiatives and systems with compliance with best practices. Applicants for funding should comply with a checklist including all the above and establish baseline requirements for resiliency, cybersecurity, interoperability. Many of these are already included in *Fiscal Year 2017 SAFECOM Guidance on Emergency Communications Grants*.[24]

[24] "Fiscal Year 2017 SAFECOM Guidance on Emergency Communications Grants," Office of Emergency Communications, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/FY%202017%20SAFECOM%20Guidance%20for%20Emergency%20Communications%20Grants_060717_FINAL508_0.pdf, accessed October 2017.

Another is to encourage and support efforts at the state level. Each state will have a different approach. A state typically has sufficient scale to make a significant difference in resiliency and security, especially if supported by funds and guidance from the federal government. A state can work with state universities to encourage and pay recently minted information security majors to work in underserved areas. It can support IT and cyber training in technical colleges with an eye to supporting government and community anchors. The state itself can set up collaborative frameworks such as mentorship of underserved counties by trained and skilled city and county CISOs.

The federal and state governments should continue to encourage and, where necessary, jump-start regional efforts. As noted, these include including support for resiliency and security efforts at councils of governments, FEMA urban areas, APCO public safety communications regions, and other regional entities.

Additionally, infrastructure initiatives developed under the White House's infrastructure plans should also include, as appropriate, communications infrastructure. The classic example is to include communications conduit and fiber alongside new or repaired roads and bridges, which can be installed at a small percentage of the cost of building that infrastructure as a standalone initiative. Others may include placing fiber and/or wireless communications within buildings.

For example, the city of Mesa, Arizona, over the period of several years, built over 100 miles of communications conduit along widened arterial and new freeway roads. The conduit was built according to industry standards and with access vaults for ready interconnection. Through coordinating with the road construction, the conduit construction was completed at incremental material and labor costs, ranging from 10 percent to 30 percent of the cost without coordination. The conduit that reaches throughout the community has been used to provide service to an industrial development near the former Williams Air Force Base, which includes the Apple global command data center. The city has also leased conduit and fiber to several telecommunications service providers, and has installed fiber for the city's use.[25]

Finally, we suggest the process map included in this Playbook be developed further to incorporate additional resources, examples, and processes beyond the scope of this Playbook.

[25] "Transcript: Community Broadband Bits Episode 139," interview with City of Mesa CIO Alex Deshuk, February 26, 2015, Community Networks, https://muninetworks.org/content/transcript-community-broadband-bits-episode-139, accessed November 2017.

Appendix A: Risk Management Process Map for Physical, Network, and Cyber Dimensions

Figure 11: Risk Management Process Map Phase I: Set Goals and Objectives

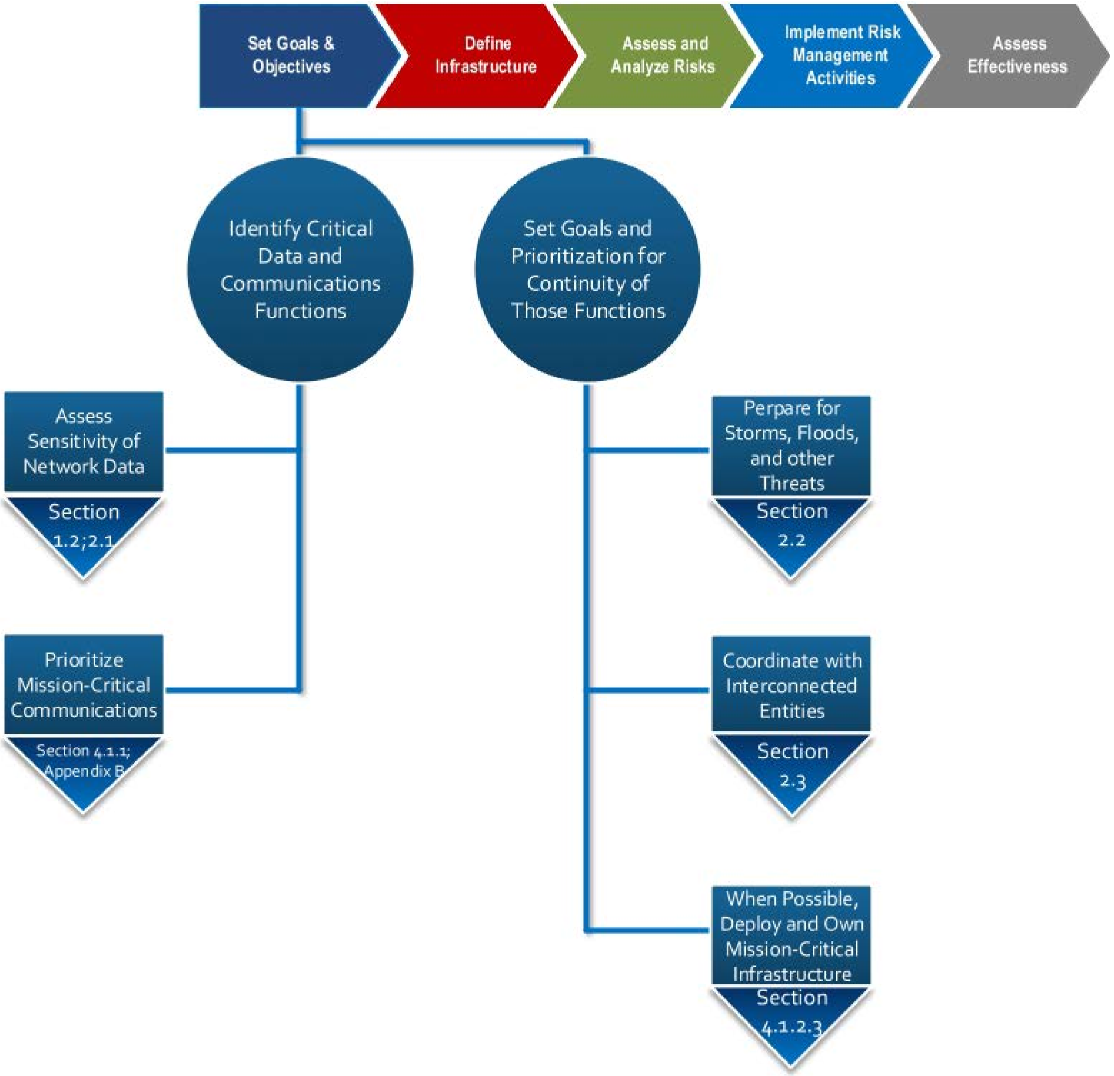

Set Goals & Objectives
Define Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness
Identify Critical Data and Communications Functions
Set Goals and Prioritization for Continuity of Those Functions
Assess Sensitivity of Network Data
Section 1.2;2.1
Prioritize Mission-Critical Communications
Section 4.1.1; Appendix B
Perpare for Storms, Floods, and other Threats
Section 2.2
Coordinate with Interconnected Entities
Section 2.3
When Possible, Deploy and Own Mission-Critical Infrastructure
Section 4.1.2.3

Figure 12: Risk Management Process Map Phase II: Define Infrastructure

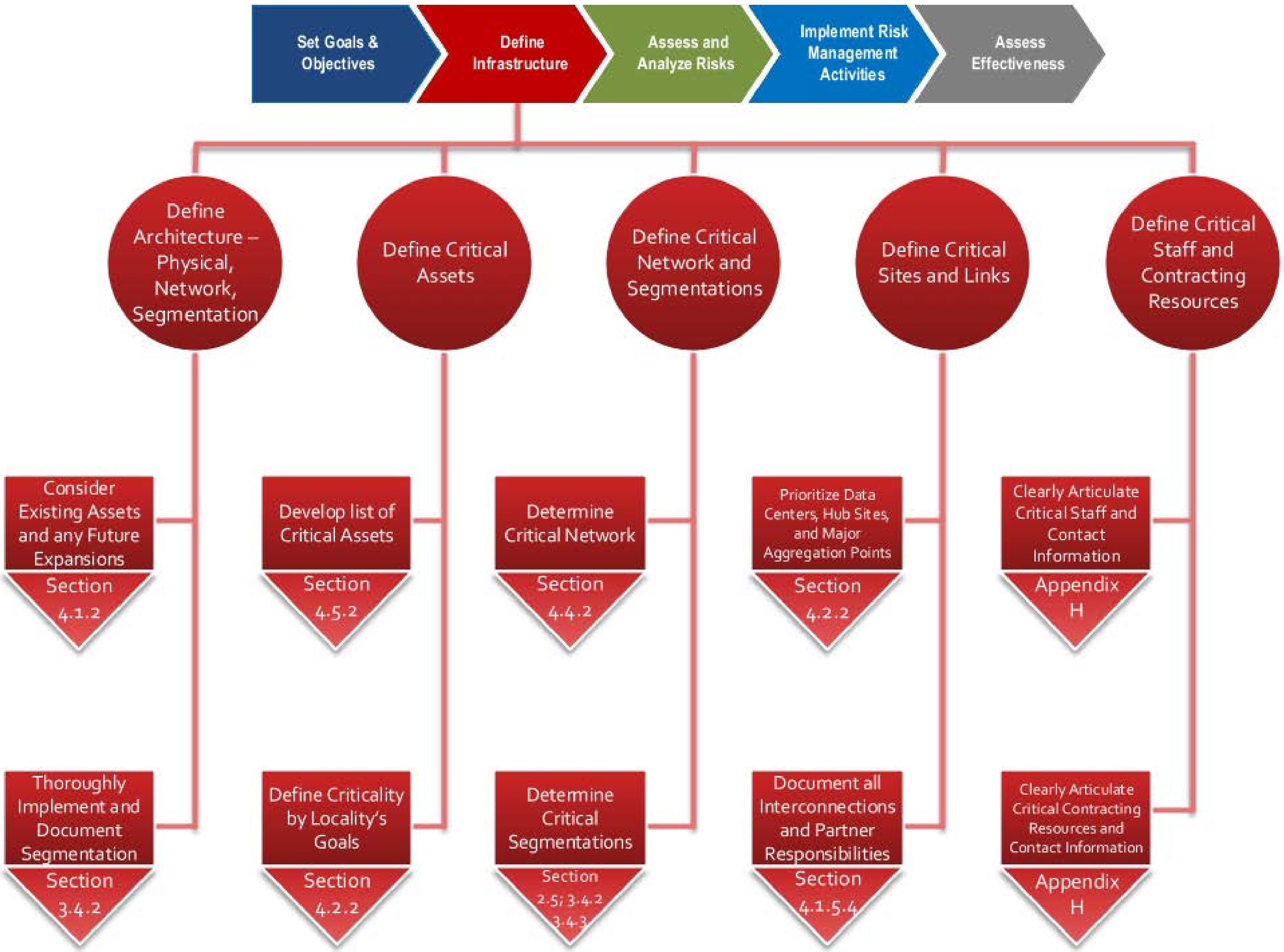

Set Goals & Objectives
Define Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness
Define Architecture – Physical, Network, Segmentation
Define Critical Assets
Define Critical Network and Segmentations
Define Critical Sites and Links
Define Critical Staff and Contracting Resources
Consider Existing Assets and any Future Expansions
Section 4.1.2
Thoroughly Implement and Document Segmentation
Section 3.4.2
Develop list of Critical Assets
Section 4.5.2
Define Criticality by Locality's Goals
Section 4.2.2
Determine Critical Network
Section 4.4.2
Determine Critical Segmentations
Section 2.5; 3.4.2 3.4.3
Prioritize Data Centers, Hub Sites, and Major Aggregation Points
Section 4.2.2
Document all Interconnections and Partner Responsibilities
Section 4.1.5.4
Clearly Articulate Critical Staff and Contact Information
Appendix H
Clearly Articulate Critical Contracting Resources and Contact Information
Appendix H

Figure 13: Risk Management Process Map Phase III: Assess and Analyze Risks

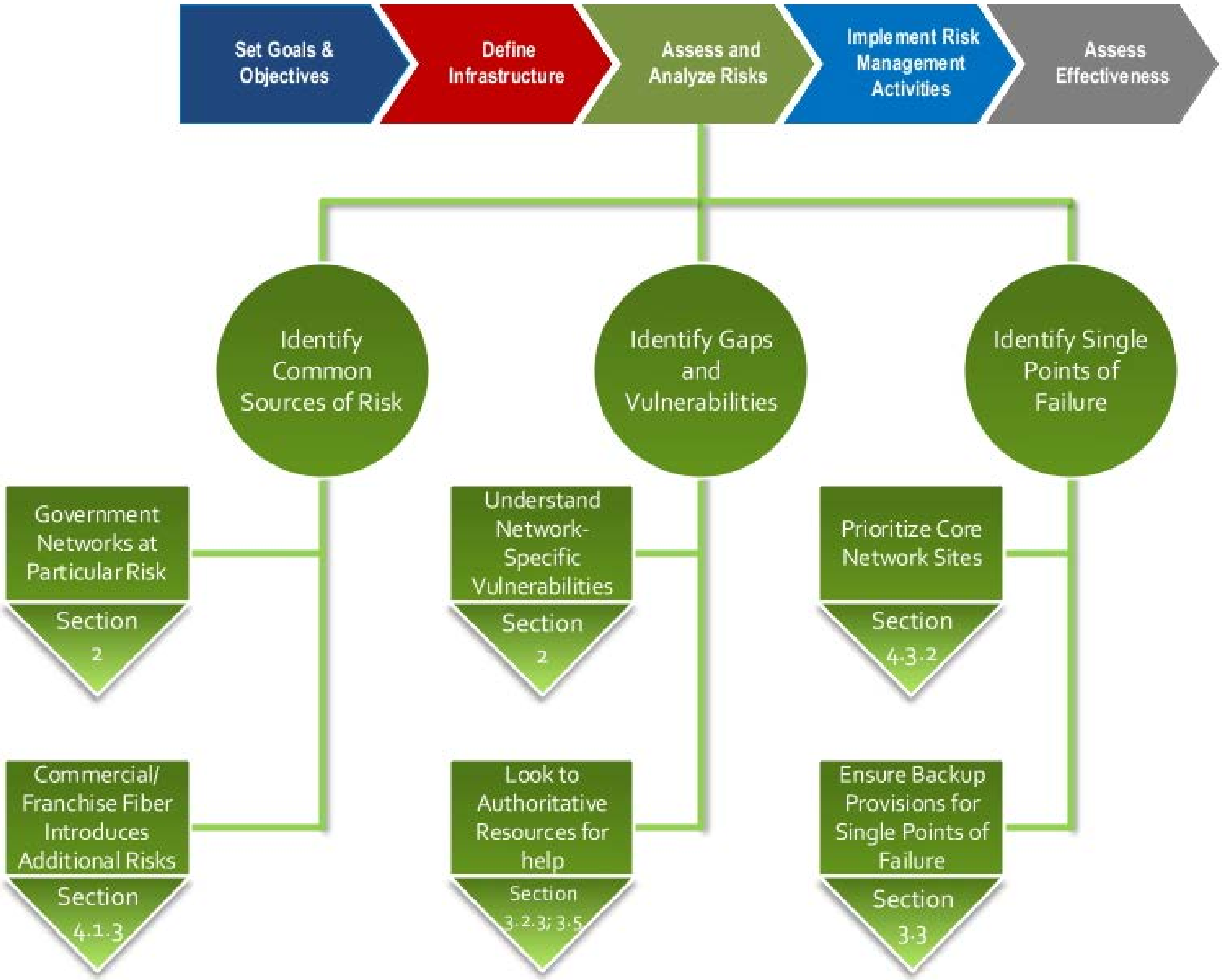

Set Goals & Objectives
Define Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness
Identify Common Sources of Risk
Identify Gaps and Vulnerabilities
Identify Single Points of Failure
Government Networks at Particular Risk
Section 2
Understand Network-Specific Vulnerabilities
Section 2
Prioritize Core Network Sites
Section 4.3.2
Commercial/ Franchise Fiber Introduces Additional Risks
Section 4.1.3
Look to Authoritative Resources for help
Section 3.2.3; 3.5
Ensure Backup Provisions for Single Points of Failure
Section 3.3

Figure 14: Risk Management Process Map Phase IV: Implement Risk Management Activities

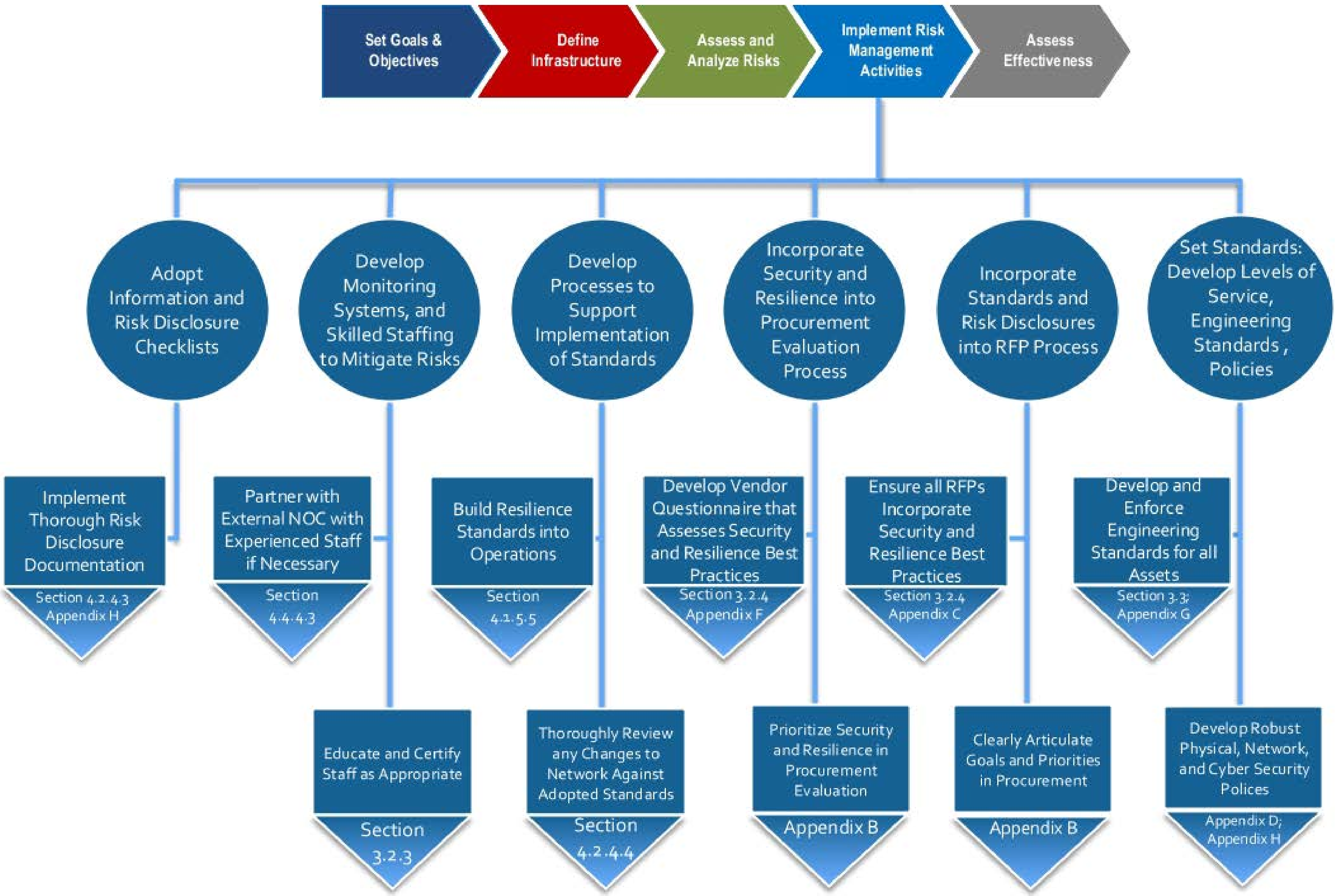
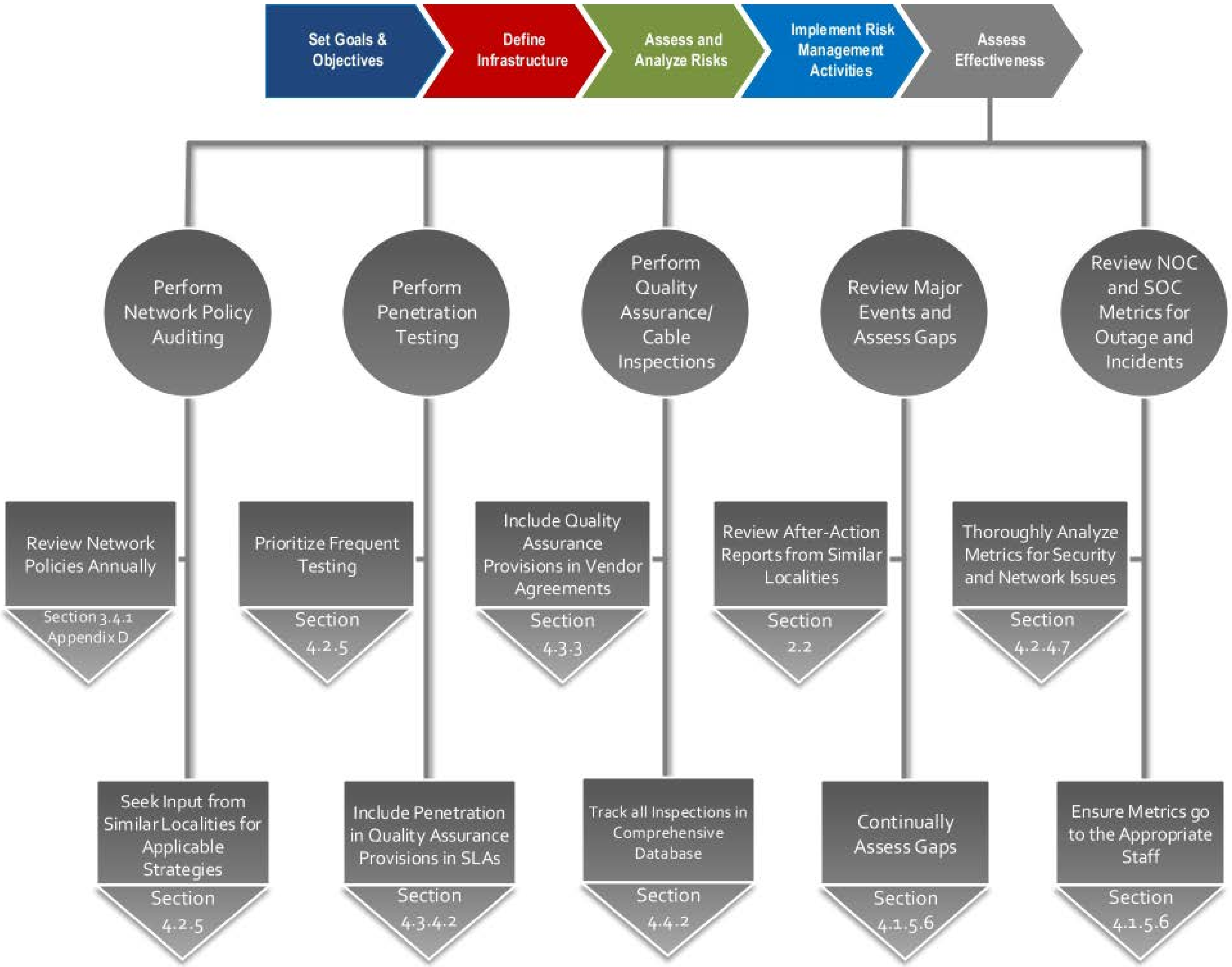

Set Goals & Objectives
Define Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness
Adopt Information and Risk Disclosure Checklists
Develop Monitoring Systems, and Skilled Staffing to Mitigate Risks
Develop Processes to Support Implementation of Standards
Incorporate Security and Resilience into Procurement Evaluation Process
Incorporate Standards and Risk Disclosures into RFP Process
Set Standards: Develop Levels of Service, Engineering Standards , Policies
Implement Thorough Risk Disclosure Documentation
Section 4.2.4.3 Appendix H
Partner with External NOC with Experienced Staff if Necessary
Section 4.4.4.3
Build Resilience Standards into Operations
Section 4.1.5.5
Develop Vendor Questionnaire that Assesses Security and Resilience Best Practices
Section 3.2.4 Appendix F
Ensure all RFPs Incorporate Security and Resilience Best Practices
Section 3.2.4 Appendix C
Develop and Enforce Engineering Standards for all Assets
Section 3.3; Appendix G
Educate and Certify Staff as Appropriate
Section 3.2.3
Thoroughly Review any Changes to Network Against Adopted Standards
Section 4.2.4.4
Prioritize Security and Resilience in Procurement Evaluation
Appendix B
Clearly Articulate Goals and Priorities in Procurement
Appendix B
Develop Robust Physical, Network, and Cyber Security Polices
Appendix D; Appendix H

Figure 15: Risk Management Process Map Phase V: Assess Effectiveness


Set Goals & Objectives
Define Infrastructure
Assess and Analyze Risks
Implement Risk Management Activities
Assess Effectiveness
Perform Network Policy Auditing
Perform Penetration Testing
Perform Quality Assurance/ Cable Inspections
Review Major Events and Assess Gaps
Review NOC and SOC Metrics for Outage and Incidents
Review Network Policies Annually
Section 3.4.1 Appendix D
Prioritize Frequent Testing
Section 4.2.5
Include Quality Assurance Provisions in Vendor Agreements
Section 4.3.3
Review After-Action Reports from Similar Localities
Section 2.2
Thoroughly Analyze Metrics for Security and Network Issues
Section 4.2.4.7
Seek Input from Similar Localities for Applicable Strategies
Section 4.2.5
Include Penetration in Quality Assurance Provisions in SLAs
Section 4.3.4.2
Track all Inspections in Comprehensive Database
Section 4.4.2
Continually Assess Gaps
Section 4.1.5.6
Ensure Metrics go to the Appropriate Staff
Section 4.1.5.6

Appendix B: FirstNet

Mobile broadband has proven vital to the majority of the nation. While the average American uses it to remain connected to friends, family, work, and an increasing amount of day-to-day tasks, first responders use it for automatic vehicle location (AVL), Computer Aided Dispatch (CAD), messaging and alerting, access to video systems (schools, highways, malls, body cameras, etc.), image/video/data transfer, incident command support, Records Management System (RMS), and even obtaining directions to their next call. These needs are becoming increasingly mission-critical and central to their jobs.

Currently, first responders use commercial mobile broadband like the general public, using Verizon, Sprint, AT&T, or T-Mobile's networks. This can be a problem when major scheduled events (concerts, rallies, large gatherings) overwhelm the network, and is particularly a problem in major incidents (shootings, terrorist attacks, mass emergencies, and natural disasters) where first responder needs are critical, the need is unpredictable, and the network may have been compromised by the incident, either deliberately (sabotage, cyberattack) or incidentally (storm damage).

To address this, some first responder agencies tried to build their own mobile broadband networks starting in the mid-2000s. As with any private network, the idea was to create an entirely separate environment that would not be affected by the public mobile broadband use. This is the model that public safety has used for land mobile radio (e.g., push-to-talk voice radios) and that is used for the private wired networks discussed in this report.

However, building private mobile broadband networks posed an almost unsurmountable challenge—first, it required sufficient wireless spectrum in usable frequencies, which were only available in a limited form on an experimental basis. Second, there was significant capital cost, both in deploying the mobile infrastructure (both cell sites and core network) and in interconnecting the sites with fiber-based communications infrastructure. Finally, there was significant ongoing cost to obtain and maintain skilled staff, and software and hardware upgrades.

Based on these early experiments including the Washington, DC area WARN and RWBN networks and others, the public safety communications community reframed this as a nationwide problem with a potentially nationwide solution—to achieve the needed economies of scale and to provide a single, interoperable network that can be used by responders nationwide.

The outcome of this solution, the federal First Responders Network Authority, or FirstNet, is tasked with overseeing the deployment of a National Public Safety Broadband Network (NPSBN) over the next five years and management of the network over the subsequent 25 years. The scale of the NPSBN is unprecedented; its ability to provide public safety users with an interoperable, secure, reliable, and resilient network remains to be proven.

Through several years of consultation with public safety agencies, states, territories, and the District of Columbia, and through an extensive vendor selection process, FirstNet sought to accomplish the following steps required for a secure and resilient network:

- Identify vulnerabilities
- Identify threats
- Determine risks arising from threats and vulnerabilities
- Prioritize risks to determine associated controls
- Specify controls to address or mitigate threats and vulnerabilities

During the life of the current contract, the success of the following is yet to be determined:

- Implementation of controls
- Effectiveness of controls
- Ability to monitor the security of the system

Below, we outline the steps already undertaken by FirstNet and those planned by FirstNet and its selected vendor to provide public safety users with a secure and resilient network that meets the technical, financial, and operational needs of first responders. The referenced documents are thorough, and offer an example of the language used in the procurement and development of a nationwide network that views the majority of its assets as "mission critical".

The Goal of FirstNet

The 2004 9/11 Commission Report[26] recommended the deployment of an interoperable, dedicated National Public Safety Broadband Network (NPSBN)—a single interoperable platform for emergency and daily public safety communications. The Middle-Class Tax Relief and Job Creation Act of 2012 ("The Act")[27] allotted high-quality 700 MHz spectrum,[28] set aside $8 billion in funds for the NPSBN and related functions, and established FirstNet under the National Telecommunications and Information Administration (NTIA) within the U.S. Department of Commerce.

[26] "The 9/11 Commission Report," https://govinfo.library.unt.edu/911/report/911Report.pdf, accessed September 2017.

[27] "Middle Class Tax Relief and Job Creation Act of 2012," Public Law 112–96, February 22, 2012, U.S. Government Publishing Office, https://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf, accessed September 2017.

[28] Known as "Band 14," representing 20 MHz of highly desirable spectrum in the 700 MHz band that provides good propagation in urban and rural areas and decent penetration into buildings.

The NPSBN, overseen by the federal FirstNet authority, will have a significant impact on how public safety communications is managed in every state over the coming decades. The potential benefits of this wireless network for public safety communications are significant. Seamless communications are expected to improve first responders' response times, increase situational awareness, and enable close integration with Next-Generation 911 (NG911) services.[29] The current focus of FirstNet deployment is on mobile data, while mission-critical voice support (mission-critical push-to-talk, or MCPTT) is projected to be deployed sometime in the future.

The promise of FirstNet is to provide first responders the ability to take advantage of data, video, images, and other information via mobile devices to more effectively save lives, more thoroughly respond to and plan for large-scale events and emergencies, and more efficiently perform day-to-day tasks. FirstNet will change the communication dynamic among emergency responders, and improve how mutual aid is organized and conducted with federal and regional agencies. Real-time video, mapping, and other unique situational awareness data are among the key applications that will enhance communications capabilities for responders, incident command, and dispatch personnel.

In 2017, FirstNet signed a 25-year contract with AT&T,[30] based on AT&T's response to FirstNet's RFP for the NPSBN, forming a public–private partnership to both build and operate FirstNet.[31] The network will comprise a national core and interconnected state Radio Access Networks (RAN's) managed either by AT&T, or by the states that choose to opt out of the AT&T network.

The complex system encompasses many layers, each with its own set of resiliency and security challenges. FirstNet, like any LTE network, is divided into: 1) a core, essentially a platform of servers that manages basic and IP multimedia functions, identity, access, billing, prioritization, and other central functions, 2) a radio access network, consisting of the cell sites/access point radios (known as eNodeBs) and the fiber transport networks connecting them, and 3) the user devices. The FirstNet enterprise also includes interconnection with Partner Networks, data centers, and public safety applications.

[29] NG911 is an Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from the public, through the 911 network, and on to emergency responders.

[30] "FirstNet Partners with AT&T to Build Wireless Broadband Network for America's First Responders," Press Release, FirstNet, March 30, 2017, https://firstnet.gov/news/firstnet-partners-att-build-wireless-broadband-network-americas-first-responders

[31] The business model enables AT&T to use excess spectrum not in use by public safety to serve "secondary" (non-public safety) users—with all revenues going back into the NPSBN—while Quality of Service (QoS), prioritization, and preemption policies will ensure that public safety users have full access to the entire spectrum as needed.

The FirstNet Special Notice and RFP

During the procurement of a vendor for deployment, FirstNet took the opportunity to solicit input from industry, public safety, and other interested parties as part of the draft RFP process in a Special Notice.[32] This Notice provided an opportunity for experts to review and comment on the Cyber Security section/requirements that would go into the final RFP was part of the consultation process.

The consensus of the expert review was:

- Security and resiliency must be built into this network from the start of the project. It is a rare opportunity to be able to do so.
- The network must follow relevant existing standards.
- The network must prepare for today's threats and tomorrow's threats as well.
- The network must be flexible, adapt to all sorts of new challenges including the incorporation of Internet of Things (IoT) technologies.

The resulting RFP laid out its objectives, dedicating an entire section to cybersecurity,[33] and security and resiliency requirements directly in targeted sections of the RFP, based on recommendations from its Technical Advisory Board.[34]

Throughout the RFP, the infrastructure requirements call for a resilient architecture and hardened sites. The National Public Safety Telecommunications Council (NPSTC), "a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership," developed a document called "Defining Public Safety Grade Systems and Facilities"[35] that has become the de-facto set of guidelines primarily for FirstNet, but is relevant for other communications systems. NPSTC recognized the need to weigh implementation of their recommendations against physical, financial, and operational factors so it notes within the document that these are goals and not "hard and fast" requirements. Given

[32] "FirstNet's Nationwide Public Safety Broadband Network (NPSBN)," FedBizOpps.gov, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=d7115b38283f9df2aa782ef5149aaff9&_cview=0, accessed October 2017.

[33] "Solicitation No. D15PS00295 – Section J, Attachment J-10, Cybersecurity," FirstNet, https://www.fbo.gov/utils/view?id=7d9982dba8e87f697802f846f08601b8, accessed October 2017.

[34] "Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network," Final Report, Technical Advisory Board for First Responder Interoperability, May 22, 2012, https://www.fbo.gov/utils/view?id=84e483ec4c9b9ced12b4da61a88a2505, accessed October 2017.

[35] "Defining Public Safety Grade Systems and Facilities," National Public Safety Telecommunications Council, Final Report, May 22, 2014, http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf, accessed October 2017.

this, the document uses "shall" and "should" to differentiate what they feel are mandatory requirements and optional, best practices.

The RFP defines public safety-grade communications qualitatively, "simply as the effect of reliable and resilient characteristics of a communications system. The system should be designed to minimize the impact of, or eliminate entirely, equipment or component failures that result in a loss of data throughput or coverage, and be designed in a manner that promotes the system's quick return to optimal performance."

This document defines, outlines risks, and documents best practices to prepare for the following:

- Environmental considerations (seismic events, wildfires, flooding, etc.)
- Service level agreements
- Reliability and resiliency
- Coverage
- Push-to-talk operation
- Applications
- Site hardening with specific requirements for physical security, antenna support structures, equipment enclosures, environmental and climate control, and power; this also includes an analysis of common practices related to site hardening conducted by commercial carriers
- Installation

Award to AT&T

In early 2017, AT&T was selected to deploy and operate the FirstNet network. In its statement to Congress,[36] AT&T stated its commitment to the security and resilience of FirstNet by:

- Certifying all devices that will be used on the network,
- Building a separate evolved packet core (EPC) for FirstNet, first responders' data will be entirely separate from other users on the network,

[36] Danny Ramey, "Senate Hearing on FirstNet Focuses on Rural Coverage, Cybersecurity," Mission Critical Communications, July 20, 2017, https://www.rrmediagroup.com/Features/FeaturesDetails/FID/769, accessed October 2017.

- Building a security operations center specifically for FirstNet that will monitor and address security threats, and
- Implementing ICAM to authenticate user credentials, and prevent any unauthorized network access

Additionally, AT&T reported to the Congressional subcommittee that it builds its towers to federal and state standards to withstand disasters such as earthquakes and tornadoes.

Physical and Network Security

FirstNet is multi-dimensional and has many potential attack surfaces, including wireless and wired infrastructure (backhaul), physical sites, applications (including the application ecosystem), and user devices.

While the network is new, and security and resiliency can be built into its infrastructure, new technologies can introduce new vulnerabilities and risks, and the network faces many unknowns until the system in operation. Because the network is not yet deployed, there is no way to know how system will perform in periods of high stress and usage, or provide the necessary security if hacked. Additionally, any cyber threats that are successful against commercial LTE will also pose a risk to FirstNet.

FirstNet operates within a radio access network (RAN) that is shared with AT&T's commercial network. This provides the advantage of using a large pool of spectrum and fiber capacity in routine and emergency operations. In addition, first responders have prioritization on the network. Public safety devices have first priority in gaining access to the network, and their communications runs more quickly than other users. If the network becomes congested, public safety use is held steady and if necessary, non-public safety use is automatically cut back.

FirstNet also has a dedicated spectrum band (Band 14) for public safety—10 MHz of capacity each in the upstream and downstream directions. In regular operation, this band is designed to be available to any user on the AT&T network. In conditions of congestion or public safety demand, non-public safety users are preempted from using the Band 14 spectrum—their use is limited to the other AT&T bands. Preemption provides the equivalent of open travel lanes for first responders only.

AT&T has promised to implement specific security and resiliency measures for FirstNet on a state-specific basis by developing State Plans.[37] At a high level, these include hardening network

[37] State Plan details are only available to state- and federal-designated personnel and cannot be disclosed.

infrastructure and backhaul, using a universal OTA protocol, and specific management practices for applications, devices, and operations.

AT&T will harden physical infrastructure “where appropriate,” otherwise it will rely on its own standards. The infrastructure is built to state and local zoning and building codes, and relies on overlapping cell site topology to cover areas where sites are down. In both planned and unplanned events, AT&T will use deployables to fill in where additional capacity and coverage are needed. For backhaul, multiple layers of redundancy are built into the core network and satellite backhaul is used for deployables.

FirstNet uses the LTE protocol, following 3GPP standards and providing priority, preemption, and quality of service to first responders. If unavailable, communications will fall back to 3G, employing multiple frequency bands to use entire AT&T-owned spectrum for necessary capacity.

FirstNet and AT&T are providing an application ecosystem that developers and public safety application buyers must use, including API toolkits, assistance to application developers, and a managed application store. AT&T and FirstNet manage device purchases, and the devices used must match specific hardware (SIM cards, etc.) protocols. All applications and devices are vetted and tested at the Public Safety Communications Research lab in Boulder, CO.

Although FirstNet is a nationwide network, each agency controls and manages their users’ access, depending on FirstNet policies specifically outlined in State Plans as well as local policies that need to be put in place which cannot conflict with NPSBN security policies.

FirstNet provides local control of priority and preemption and of which users are permitted to have accounts and use of the network. Local incident managers determine who has access to the network and who attains what level of priority in an incident. Although the prioritization function is designed to be automated, FirstNet is essentially developing a manual override that can address specific needs in an emergency and provide capacity to particular applications, responders, and groups of users.

It is important to understand the distinction among levels of FirstNet users. Primary users are law enforcement, fire and emergency medical services personnel who will always have priority on the network and will, when needed, preempt (kick off) non-primary users. Extended Primary users are additional personnel who are needed during emergency situations (e.g., utilities, hospitals, transportation, etc.). Extended primary users will always have priority on the network and can be elevated to have preemption during an event. The different types of users will have varying needs depending on the situation.

Assessing Effectiveness and Learning from Other Networks

FirstNet continues to adapt its strategies, based on the ongoing experiences of statewide "early builder" mobile broadband public safety networks. In recent years, early building networks including those in Los Angeles; New Jersey; Harris County, Texas; New Mexico, and Adams County, Colorado have deployed prototype LTE public safety networks that have proven some best practices. Characteristics of a successful early builder network include:

- Effective governance
- Inclusion of local agencies in planning, design, deployment and decisions; constant consultation
- Sufficient performance, especially coverage and capacity
- Affordable cost structure for both the state and local agencies
- Interoperability
- Satisfactory and appropriate training
- Planned and unplanned maintenance by trained technicians
- Thorough, specific, and well-documented policies
- The guarantee of a network that meets the highest standards for security and resiliency

FirstNet continues to learn from Broadband Technology Opportunities Program[38] (BTOP)-funded public safety networks nationwide:

> "The Broadband Technology Opportunities Program (BTOP) administered by NTIA provided funding for seven public safety projects in 2010. These funds were partially suspended two years later, after Congress enacted the law creating FirstNet. The suspension was needed to ensure that any further activities would be consistent with the mandates of the new law. FirstNet reviewed the proposed BTOP projects and determined that there was value in continuing to support them. As a result, FirstNet reached spectrum manager lease agreements with the Los Angeles Regional Interoperable Communications Systems Authority (LA-RICS), Adams County, Colorado (ADCOM-911), the State of New Jersey and the State of New Mexico.
>
> "FirstNet will provide technical support to these BTOP projects and will share any lessons learned with the broader public safety community to enable the successful implementation of FirstNet's nationwide deployment."[39]

[38] BTOP was an initiative within the American Recovery and Reinvestment Act of 2009 (ARRA) stimulus program.

[39] "Guiding Principles," FirstNet, https://www.firstnet.gov/content/firstnet-will-support-and-learn-its-btop-project-partners, accessed October 2017.

In addition to these BTOP projects, Harris County, Texas, using its own funds, deployed a stand-alone public safety LTE broadband network.

Lessons learned from these projects helped solve some of the puzzle for FirstNet. Each of the BTOP recipients, in exchange for the use of the broadband spectrum, documented Key Learning Conditions Plan(s) (KLCs). Examples of these projects include:

- LA-RICS designed and deployed a 74-site multi-agency network covering a highly urban area. It has been used successfully during the Rose Bowl parade for the past two years.
- The State of New Jersey developed JerseyNet, a system made up entirely of deployables (mobile base stations and cores) that can enhance coverage and/or capacity or replace a persistent system entirely if lost. It has been deployed successfully to multiple events in and around New Jersey, including the visit of Pope Francis to Philadelphia, the Atlantic City Beach and Air Shows, the Miss America Pageant, the PGA Championship at Baltusrol Golf Club in Springfield, the 96th Annual Far Hills Steeplechase, the Millville Airshow, and the Princeton University Alumni Weekend. JerseyNet assets were also deployed to Florida immediately after Hurricane Irma to provide additional communications to first responders.
- Adams County, Colorado, had the first operable public safety broadband BTOP-funded network in the country, including the implementation of an Enhanced Packet Core (EPC) —the ‘central nervous system’ of the network—providing guidance to each of the other projects and to FirstNet.
- The State of New Mexico’s LTE network interfaced with the remote core in Adams County determining technical, schedule and cost considerations when doing so. They also utilized New Mexico’s middle mile infrastructure for backhaul, and provided a test bed for architecture concepts along the U.S./Mexico border area which included developing operating procedures for join use among federal, state, and local authorities.
- Harris County developed and deployed a countywide LTE broadband network that was put to the test during the Houston-hosted Super Bowl. The after-action report has been widely circulated and provides incredible insights into not only the operational logistics, but also the ability of such a network to identify, track and apprehend offenders.

Appendix C: Sample Procurement Document for Fiber Network Design Engineering

Procurement Document

For a Fiber Network

Released: [Date]

Contents

1 Summary

The Locality ("Locality") is seeking proposals from qualified contractors ("Respondents") to design and engineer a network. The network shall serve [Insert Area]. Where possible, the network will utilize and extend from existing Locality-owned fiber infrastructure.

The design and engineering scope shall be limited to the physical layer of the network, including fiber optic cable, conduits, connectors, and related components, but does not include network electronics.

Due to the technical nature of the services sought and the need for a contractor with a proven record of quality, the Locality has determined that the procurement of network design and engineering services is best accomplished by utilizing a [RFI/RFP/RFQ] process. Such process will enable the Locality to evaluate key factors impacting the successful completion of this project, such as the Respondent's relative experience and past performance with similar projects. The Locality intends to select the most advantageous proposal on the basis of the overall value proposition it represents in terms of total cost, quality of workmanship, and timeline.

The Locality expects, based on previous studies, that the majority of the infrastructure will be built using [underground/aerial] construction methods. In total, we estimate approximately [total number of] route miles of fiber plant passing [total number of] service locations will be required, not including FTTP service drops. The Locality does not guarantee the accuracy or validity of the assumptions used.

The awarded Contractor will be required to perform all work described in, and in accordance with this RFP. The preferred Respondent will demonstrate prior experience working with government agencies developing next-generation communication networks for broadband access, with particular expertise in preparing FTTP network designs, and fiber optic outside plant design and engineering.

2 Project Background

- [Discuss goals of Locality's project]
- [Discuss benefits of deploying infrastructure in Locality]
- [Discuss existing communications assets]
    - [Include map of existing assets, if possible]

3 Statement of Need

The network design and plan must accommodate the Locality's broadband network requirements and project goals. The project scope is based on [discuss scope of deployment], with provisions for a fiber connection to [total number of sites], and diverse connections from the network hub to [total number of critical sites].

All interested entities are strongly encouraged to respond. We welcome the responses of incumbent service providers, competitive providers, non-profit institutions, and public cooperatives.

General Network Considerations

1. The network should pass [areas, sectors, total number of passings].
2. The network shall operate from a network Hub facility located on Locality-owned property.
3. The network shall connect to the following [critical sites]:
   - [123 Main St.]
   - [456 Broadway.]
   - [789 Courthouse Cir.]
4. The network should be capable of supporting a range of standards-based access technologies, including Active Ethernet (IEEE 802.3) and Gigabit Passive Optical Network (GPON) technology, as well as higher-speed emerging standards (XGS-PON, NG-PON2, etc.). The network should be designed for high levels of redundancy, reliability, and resiliency.
5. The network should be expandable in a manner as efficiently and effectively as possible to increase data capacity, expand the service area, and to accommodate advances in technology as may reasonably be expected to become available over the life of the network (at least 20 years). Specifically, the network should allow for future expansion so that service to homes, businesses, institutions, and public buildings can be provided throughout the Locality.
6. The network should be constructed with additional spare strands to allow for leasing dark fiber to non-Locality entities (open access). [If desired]
7. The design should provide controlled physical access to all equipment and facilities.

The design is limited to the physical layer of the network (conduit, fiber, etc.), and does not include network electronics, but must take into account current and emerging network technologies.

For the network to have the intended economic and quality of life impacts, we consider both cost and availability of service to be important. We encourage responses that address both to maximize adoption of the service.

Network Design and Engineering Parameters

The following baseline technical attributes are preferred:

- Fully fiber-based connectivity to all sites;
- Fiber design that meets applicable physical layer specifications defined by the ITU G.984 standards in order to enable GPON technologies and emerging, higher-speed PON technologies;
- Fiber strand capacity and physical architecture (e.g., handhole placement, backbone routes, etc.) anticipating future ubiquitous deployment to all homes and businesses;
- Fiber routes that are aligned with existing Locality conduit and coincide with planned Locality utility, roadway, and related capital improvement projects to reduce cost and minimize disruption where possible;
- Low latency;
- Backbone topology capable of supporting connections over diverse paths from one or more central hub locations to fiber distribution cabinets located throughout the area to facilitate high-availability service offerings;
- Primarily underground construction utilizing directional boring as the main construction methodology;
- Fiber distribution plant placed in underground conduit (as opposed to direct burial cable) to more readily facilitate repairs and capacity upgrades;
- Minimal use of micro-trenching and rock sawing, which are not preferred construction methodologies.
- Underground fiber distribution plant placed in 2-inch conduit (as opposed to direct burial cable) to more readily facilitate repairs and capacity upgrades;
- Handholes spaced no more than 500 feet apart along backbone routes, and spaced optimally along distribution routes to serve passings in the most efficient manor; and
- Active components placed in environmentally hardened shelters and/or cabinets equipped with backup power generation and/or batteries, as appropriate, capable of sustaining services in the event of extended power outages;
- Fiber path diversity to public facilities to maintain continuous service even if one path is broken;

4 Scope of Work

The awarded Contractor will be required to provide the design, engineering, permitting, and full construction documentation for the network. All documentation shall be provided in electronic and printable format. This work will include, but not be limited to, the following tasks:

1. Develop system-level network designs;
2. Perform field walk-out and documentation of all fiber routes;
3. Prepare detailed, GIS-based designs and CAD construction prints of final designs;
4. Prepare a bill of materials;
5. Provide construction specifications;
6. Determine and document make-ready requirement;
7. Determine and document permitting requirements;
8. Provide recommended phased construction approach and time-line which will include an FTTP pilot service area.

The Contractor shall provide a primary point of contact to the Locality for the duration of the contract, and shall be expected to attend regular project status and management meetings.

Task 1 – Design Services

The Contractor shall develop a conceptual design for the network in accordance with the goals and objectives expressed in this RFP. The design is limited to the physical layer of the network (conduit, fiber, etc.), and does not include network electronics, but must take into account current and emerging network technologies. It is the intent of the Locality for the physical infrastructure to support any current or future mix of Passive Optical Network (PON), Active Ethernet, and/or future technology standard.

The Contractor shall initiate this effort by facilitating a kick-off meeting with the Locality and other advisors to establish key project parameters. Specific agenda items will include, but are not limited to:

- Review and refine the project scope of work;
- Establish the project schedule;
- Assign project points of contact and define communications protocols, including progress reporting expectations and formats;
- Review and collect existing infrastructure documentation;
- Discuss the anticipated network operating model and corresponding impacts to the design strategy;
- Define technical and functional design objectives for the network; and
- Establish processes for Locality review of engineering and permitting.

The Contractor shall prepare a system-level design, including applicable schematics and material specifications, identifying key system-level parameters impacting later design phases, such as the type and quantity of fiber optic components and related components (termination panels, connector types, splice enclosures, etc.); proposed fiber routes; and the general suitability of candidate hub locations to support passive and active fiber network components.

The Contractor shall prepare a conceptual design consisting of preliminary fiber routes; identification of hub location(s) and functional requirements; logical backbone network schematics; a reference design encompassing all key design parameters for all applicable network layers; and a preliminary bill-of-materials (BOM) and cost estimate.

Task 2 – Detail Design and Permitting Services

The Contractor shall produce final network designs based on Locality-approved conceptual designs.

The Contractor shall prepare complete engineering packages for new outside plant fiber routes to include:

- Engineering detail sheets/"typicals" (i.e., the standard set of required construction parameters, covering details such as methods for utility pole attachment, depth of trenching, and type of handhole specifications; which will accompany all engineering prints)
- GIS-based network maps
- Permit submissions/CAD engineering prints
- Material specifications
- Bill of Materials (BOM)
- Splice matrices
- Network logical ("stick") drawings

Task 2a: Field Surveys

The Contractor shall conduct a field verification and refinement of preliminary fiber routes. The Contractor shall capture field data and measurements in a format that can be directly imported into GIS databases, and should document all required information to produce permit-ready engineering drawings, including but not limited to:

- Storm drains
- Edge of pavement
- Water and sewer lines
- Slack storage
- Splice cases

- Vault/handhole locations
- Required hardware
- Utility pole location, number, and class
- Residential and/or business building entry points
- Private roads and rights-of-way

The Contractor will note potential barriers to construction, as well as potential route improvements, and will also determine what permits will be needed to install the fiber.

Task 2b: Preliminary Design of Routes

The Contractor shall provide preliminary engineering designs for the Locality review and approval, to include, but not limited to:

- Running line of fiber
- Road names
- Railroads and crossings
- Fixed markers/significant landmarks (e.g., fire hydrants, valves, poles)
- Environmental protected areas (e.g., wetlands, bodies of water)
- Flood plains
- Easements
- Rights-of-way
- Fiber cable type and placement
- Any applicable public utilities or assets
- Any applicable private utilities or assets
- Termination points
- Fiber entry and installation, as applicable

Task 2c: Permitting

The Contractor shall determine all permits required for construction of the network, to include any right-of-way encroachment permits, utility easement modifications, and/or applicable environmental permitting required.

The Contractor's engineering designs shall identify any areas in which environmental permitting may be necessary to avoid impact to the network design.

The Contractor shall document all required permits and applications requirements.

Task 2d: Final Design of Routes and Completion of Engineering Work Documents

The Contractor shall provide completed designs and permit application documentation to the Locality for review and approval. The Locality anticipates this will occur on an ongoing basis in parallel with preliminary design efforts. Furthermore, draft Engineering Work Documents (EWDs) shall be provided by the Contractor during the Material Take-Off (MTO) process for review and approval by the Locality and/or the Locality's representative prior to finalizing the Bill of Material (BOM) for procurement.

The Contractor shall produce final "Issued For Construction" (IFC) EWDs, including an updated BOM, updated cost estimates, proof of permit issuance, and all required engineered drawings, splice matrices, and design specifications.

All revisions to IFC documents after the initial issue shall be handled using best "change management" practices to assure that the Locality and all parties included on the EWD distribution list receive copies of the revised documents in order to keep all document sets current and up to date. A brief summary of the change, and reason for the change, for each document revision shall be provided along with the revised document(s).

A complete list of all EWDs and the current revision number and issue date shall be maintained throughout the project in Excel format and be available both electronically and in hard copy with the "Field Master Drawing Set".

Assistance in developing RFB for construction contractors

The Contractor shall assist in creating the construction request for bid (RFB) documents based on its completed design and engineering deliverable and the Locality's procurement regulations. During the construction bid period, the Contractor shall be available to answer questions from bidders about the RFB documents.

5 [RFI/RFP/RFQ] Response Requirements

The Locality requests the following information—in as much detail as is practicable—from respondents:

1. **Cover Letter:** Please include company name, address of corporate headquarters, address of nearest local office, contact name for response, and that person's contact information (address, phone, cell, and email).

2. **Affirmation:** Affirm that you are interested in this partnership and address the core project goals and requirements listed above. If you cannot meet any of those requirements, indicate the requirements to which you take exception and provide an explanation of the exceptions.

3. **Experience:** Provide a statement of experience discussing past performance, capabilities, and qualifications. Identify other networks your firm has designed, built, maintained, or operated; include types of materials, architectures, and unique

capabilities or attributes. Discuss partnerships with other service providers, governments, or nonprofit entities you have undertaken. Describe the nature of the projects and your firm's role. For entities currently providing communication services in or near the Locality, describe your current service footprint in the Locality, including a description of the type of infrastructure and services you currently offer and the technology platform(s) used. Explain how your firm is a suitable partner for this project.

4. **Contractor's Management Plan:** Describe your approach to staffing, project management, and subcontracting, to include:
   - Project Management Plan describing tools and procedures used for tracking, reporting, and customer communications;
   - Staffing plan describing key roles and responsibilities, including an organizational chart of key team members;
   - Subcontracting plan indicating the specific roles of proposed sub-contractors, as well as your past relationship and project experience with any proposed subcontractors;
   - Quality control plan that identifies techniques, policies, and procedures for internal quality control at all stages of the design process.
5. **Schedule:** What is your proposed schedule for design and engineering? Offer a timeline with key milestones.
6. **Proposed Pricing Forms and Rates:** Describe pricing for services described in this [RFI/RFP/RFQ] in reference to the Scope of Work outlined in Section ⍰.
7. **References:** Provide a minimum of three (3) references, including contact information, from previous contracts or partnerships.

6 Response Process

All correspondence regarding this [RFI/RFP/RFQ] should be directed to the Locality [Contact title]:

Name
email address

The Locality cannot guarantee that correspondence directed to other Locality staff or departments will be received or considered.

1. **Letter of Intent:** All interested respondents are asked to submit a letter of intent via email by **DATE** to NAME at email address.

2. **Questions:** Questions related to this [RFI/RFP/RFQ] should be emailed to email address no later than **4:00 PM EDT on DATE, YEAR**.

3. **Response Deadline:** Final [RFI/RFP/RFQ] submissions must be received in electronic form by **4:00 PM EDT on DATE, YEAR**. Please send [RFI/RFP/RFQ] response by email in PDF format to email address.
Please identify any proprietary and/or confidential information as such.

4. **Summary of [RFI/RFP/RFQ] Process Deadlines:** The following is the schedule for responding to this [RFI/RFP/RFQ]. The schedule is subject to change:

   DATE, 2017 – [RFI/RFP/RFQ] issued
   DATE, 2017 – Deadline for submitting letter of intent to respond to [RFI/RFP/RFQ]
   DATE, 2017 – Deadline for submitting questions
   DATE, 2017 – Responses to questions due (from Locality)
   DATE, 2017 – [RFI/RFP/RFQ] responses due

The Locality thanks you in advance for your thoughtful response.

7 Personal Presentations

At its discretion, the Locality may request that Respondents that provide a timely response to this [RFI/RFP/RFQ] make an individual and personal presentation to better explain information or solutions identified in the response. These presentations, if requested by the Locality, shall be held at a time and place of mutual convenience.

Appendix D: Sample Internet Use and Regulations Policy (Arlington County)

Subject/Topic: Electronic Communications and Internet Services

Topic Category: General

Department Lead: Department of Technology Services, Office of the CIO

Summary: To define the Internet Use Policies (IUP) for all Arlington County Government employees, contractors, consultants, constitutional employees, temporaries, and volunteers. These policies define access to and use of these services and ensure that their use is consistent with County policies, applicable laws, and the individual user's job responsibilities. These resources are provided by the County to enhance the ability of the user to perform job duties, improve customer service, increase productivity, reduce paperwork and provide opportunities for professional growth through approved webinars and training.

1. **Purpose:** This policy is designed to protect the County's computer networks and data assets against unauthorized and malicious use as well as to prevent potential misuse of County resources. These policies recognize that efficient use of these resources may:

   - Enhance partnership, community involvement and the exchange of information and ideas among citizens, businesses and local government.

   - Provide information both internally and to the public about the activities and services of the County.

   - Improve the quality, productivity and general cost-effectiveness of the County's work force.

2. **Scope:** The scope of this policy is limited to electronic communications and internet services. This policy covers County "networked resources," which for purposes of this policy includes the County's email system, network, software, applications, databases, internet/intranet access, all computer systems, internally hosted or cloud-based, hardware, temporary or permanent files and any related systems or electronic devices authorized personally owned or leased by the County and/or made available to employees or other authorized users (as defined in Section 2) in their role as employees or authorized users.

Internet services include the following:

a. Internet access and usage. Internet access is defined as the ability to connect to the Internet and to access the Internet.

b. Electronic Messages sent using the County's domain as well as sent through the Internet. This policy is applicable to e-mail, text messaging, social media posts, messages sent to list services, user groups and other Internet forums.

c. VPN – Use of Internet resources while connected through a Virtual Private Network.

d. Installation of Network devices. Appliances such as routers, hubs, switches, wireless access points, or other devices which facilitate authorized access to County servers, messaging systems or the Internet.

e. Social Media. This policy supplements the County's regulations regarding social media use and maintenance of web sites.

f. Calendaring. The electronic systems provide a scheduling function whereby employees may schedule meetings with each other and non-County personnel. Calendaring capability also provides for the reservation of resources such as conference rooms and equipment.

3. Roles and Responsibilities:

The Chief Information Officer (CIO) and the various sponsor groups of his/her peers from the Executive Leadership Team and Constitutional Officers have managerial responsibility for the technology initiatives contained in this regulation. The CIO is responsible for reviewing and approving any exceptions to this policy.

Department of Technology and Information Services (DTS)

DTS is responsible for providing, administering, and insuring security and records management compliance of messaging services, as well as a secure Internet/Intranet connections.

County networked resources are intended for County government business purposes only. Therefore users (as defined in Section 2) must adhere to this policy. If in doubt, the burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to accessing network resources. Questions concerning whether a particular use is acceptable or unacceptable should be referred to the department director, delegated representative or the DTS Service Desk.

Users are expected to know how to manage records in an electronic messaging system and to comply with County's records retention policies. Questions related to records retention should be directed to the DTS Service Desk.

4 . **Ownership and Privacy**.

All information created, generated, transmitted, and stored by users is the property of the County. It is not considered private. The County reserves the right to set or restrict permissions and accessibility rights to all data resources as it deems necessary. The Chief Information Security Officer (CISO) will authorize access to data stores upon written request.

5. **Access and Monitoring.**

There is no expectation of privacy when using County networked resources whether those resources are locally hosted or cloud-based. The County reserves the right to monitor and/or log all network activity with or without notice, including messaging and all web communications. The County will not monitor individual messaging or device tracking without proper approval following established County processes.

However, in the routine course of technology administration, the County undertakes construction, repair, operations and maintenance of messaging systems that may occasionally result in accessing random transmitted or stored messages. County servers also maintain logs of Internet activity, i.e., sites accessed by users and Internet traffic. County servers also maintain logs reflecting messaging traffic, i.e., to whom messages were sent and received; including external destinations. Monitoring of a specific activity, or an individual's use, may be performed without consent or knowledge of the individual only under the following circumstances and only when authorized by the County Information Security Officer. By way of example, not limitation, monitoring and/or access may be authorized:

- If required by law or in defense of a charge, claim, notice of violation or lawsuit.
- When reasonably necessary to investigate a possible violation of a County Policy, breach of security or in support of a FOIA related request.
- When there is reasonable suspicion that a user has committed or is committing a crime.

- If there is a suspected violation of this policy, of any Administrative Regulation and/or to investigate claims made against the County, the CISO will notify the Office of the County Attorney.
- To comply with the requirements of the Virginia Freedom of Information Act and the Virginia Public Records Act.
- To comply with any Litigation Hold requirements or legal discovery requests.
- To resolve a technical problem.

6. Acceptable Uses:

1. Network resources shall be used:

a. In the pursuit of County goals, objectives and activities. Official County business conducted via networked resources and electronic communications shall comply with all statutory requirements;

b. When electronic communications are the most efficient and/or effective means of accomplishing the County's business;

c. For County work-related job responsibilities, research, activities and/or information gathering;

d. Using utility and applications software that accomplish tasks and fulfill job functions that are under provided under a license issued to the County;

e. To facilitate communication and collaboration between staff and/or other appropriate entities or persons; and/or

f. To support the professional activities or projects of users (e.g., electronic scheduling of meetings, electronic calendars, project management software, address books and completion of work related forms electronically) that support the user’s official County responsibilities and job duties.

2. Incidental and reasonable personal use is permitted so long as it does not interfere with the conduct of a user's work, the effective delivery of services, incur cost to the County, generate more than incidental traffic or networked

resources, and/or conflict with Unacceptable Uses (stated in Section 9). This limited personal use of County networked resources is best accomplished during breaks and lunch time or to address critical personal matters.

3. When using electronic communications provided by Arlington County, employees are representing the County government and should conduct themselves as County government representatives at all times. Electronic messaging is considered an official communication of County government. In addition:

- Only signature lines that provide an employee's name, title, physical address and contact information should be appended to any email sent in furtherance of County business or sent through County networked resources.

- "Tag-lines" that are unrelated to the users work functions are not permitted.

4. Care must be taken when handling confidential information. Confidential information contains Personally Identifiable Information (PII) including financial information, proprietary information, social security numbers, credit card or bank account numbers; health records and personally identifiable health information. Such information should be sent via encrypted messaging and stored encrypted when at rest. If sent internally, such messaging should be limited to a "need to know" basis and sent in accordance with department procedures in effect at the time of transmittal. All such messaging should be marked "confidential" and no Personal Identifiable Information (PII) should be included in the subject line of email or posting in social media applications.

5. Use of network resources must conform to the County's anti-harassment and discrimination policies as stipulated in Administrative Regulation 2.7 addressing Personnel Rules.

7. **Unacceptable Uses**:

Unacceptable uses include, but are not limited to, the following:

a. Interference with the security or operation of County networked resources including, but not limited to, sabotage of or vandalizing any County or Internet hardware, software, network or data file.

b. Deliberate introduction or distribution of computer viruses, malware, or spy ware such as keystroke logging tools.

c. Use of network resources beyond the uses outlined in Section 8 or copying, sale or distribution of networked resources.

d. Alteration of County-provided Internet access configurations in any way except as authorized in writing by the director of DTS.

e. Unauthorized use of copyright protected works including software, electronic files (including, but not limited to, messages, e-mail, text files, image files, database files, sound files and music files), movies or data or making available copies of such works or files using County government-provided electronic communications services. Permission from the owner for the use, distribution or copying of such information must be properly documented.

f. Except as may be necessary for the performance of the user's job, access to, generation, transmission, receipt or storage of information that is abusive, discriminatory, harassing, associated with gambling or has sexually explicit content as set forth in Virginia Code Section 2.1-804 as amended.

g. Unauthorized access to County data intended for internal operations in support of non-county activities related to outside employment or personal gain.

h. Unauthorized access to materials, systems or files that are restricted by law or County policy.

i. Release or distribution of confidential information required by law or policy.

j. Representation of oneself with an anonymous or fictitious name or hosting a personal web site on a County server.

k Transmission of chain messages.

l. Transmission of global (meaning to all users) or mass (appropriate number of users to be defined by agency head) e-mails, even when the content is related to County business must be authorized by the Communications Office (County Managers Office). Department directors, or designees, may authorize employees to send messages related to County business to all members of a work or organizational group, or team that exceeds 50 users.

m. Any activities unrelated to County business in the pursuit of profit or gain for the user or on behalf of any other individual or organization.

n. Unauthorized access of County data intended for internal operations or any use of this data for political activities such as, but not limited to, solicitation of funds, or endorsement or advocacy of any particular candidate or political party.

o. Storage of County data on third-party (SaaS or cloud) applications (including, but not limited to, file storage and sharing services such as Dropbox) without prior approval from DTS.

p. Storage of County data on personal devices or media, if the device or media does not have Mobile Device Management software installed and activated.

q. Storage of official County records in applications that have not been approved by the Chief Records Management Officer, or storage of official County records on media that is not backed up on a routine basis.

r. Violating the rights of others by publishing or displaying any information that is defamatory, obscene, known to be false, inaccurate, abusive, profane, sexually oriented, threatening, racially offensive, and considered to be bullying or otherwise biased, discriminatory or illegal or otherwise insensitive forms of humor.

s. E-mail or social media discussions involving any subject that interferes with work or where items are debated at length.

t. Unreasonable work time surfing the Internet, as determined by the employee’s job functions and the task involved.

u. Misrepresenting one’s position in the County for activities unrelated to official County business.

v. Using County networked resources for private consulting or personal gain.

w. Uses that violate County warranties or terms of use for County-provided devices or software.

x. Forwarding (bulk or individually) of County official email accounts to personal email accounts without prior authorization from the CISO.

y. The use of or installation of routers, hubs, switches, wireless access points, Internet of Things (IoT) devices, etc., without authorization from DTS.

z. Use of technology to capture and record video and/or audio content where privacy is presumed or where such use has not been authorized.

8. Compliance with Copyright, Licensing and Terms of Use:

Users are required to honor copyright laws of any materials and all site or software terms of use and licensing restrictions. Software piracy is both a crime and a violation of County policies. Illegally reproducing software may be subject to criminal and civil penalties as well as disciplinary action. In no instance shall any user disassemble, reverse engineer or otherwise reproduce any software or code provided by the County. Further, all software must be used strictly in accordance with its license agreement, including any restrictions on the number of users.

Please be aware that many copyright and licensing restrictions do not allow a person to store copies of a program on multiple machines, distribute copies to others via disks or Internet or to alter the content of the software unless permission has been granted under the license agreement. Most times, supervisory permission is also required by the County. If copyrighted material is downloaded, it must be with permission of the owner and its use must be strictly within the agreement as posted by the owner, author or otherwise in accordance with current copyright law.

9 . Virus protection:

The County's standard anti-virus software must be installed on County PCs prior to accessing County networked resources. DTS is responsible for the installation of virus protection software on PCs that departments purchase. In the event updates do not occur successfully, users must contact the DTS HELP DESK (ext. "4357") to open a trouble ticket so that the updating process can be re-established.

Any virus detected must be reported to the DTS HELP DESK

10. Security:

County users are responsible for their Email and Social Media accounts. To ensure security compliance, users are prohibited from using another person's user ID, password, files, systems, even if that person has neglected to safeguard his/her user ID. Users are specifically prohibited from messaging under another user's name or spoofing another individual's identity.

Employees, contractors, or vendors responsible for connecting outside networks to the County's network are liable for any damages which may occur as a result of the connection. Safeguards such as Firewall protection, VPN, Data Loss Prevention, Encryption, and other security technologies must be provisioned and authorized by DTS. DTS must be notified prior to any connection between a non-county and county-network. Every department that uses the County's Internet gateway must be authorized and registered through DTS. Every "device" or "host" connecting to the Internet must have a unique identifier assigned by DTS.

Internet security protocols can be compromised. Users should assume that all transmissions over the Internet via e-mail, the Web, or other media, such as file transfer protocol (FTP), are publicly available, and individuals other than the intended recipient(s) can intercept such information (reference Section 8.4).

When working remotely users must ensure their telework device have updated anti-virus and firewall software operating on their telework device.

When using wireless routers for telework users must activate password protected access as well as transmission encryption (example WPA2).

When using Mobile Devices (such as iPhones, iPads, etc.) the user must ensure the device has DTS enabled Mobile Device Management (MDM) installed and activated. If any smart device (County or BYOD), which contains County information is lost or stolen the user must notify DTS Service Desk within 24 hours (Reference DTS MDM policy).

Password protection of all electronic devices is required. All users shall be required to change network access passwords in a manner and time as determined by DTS. Passwords are not to be shared or otherwise distributed by any user except as authorized. Passwords must be changed every 90 days without exception.

Contractors who may have access to County Confidential Information shall be required to sign the County's *Nondisclosure of Data and Security Agreement* prior to commencing work under any County contract.

The provision of new applications must comply with DTS Information Governance requirements as defined by the CISO and Chief Records Management Officer (CRMO).

11. Access violations:

It is a violation for any user, including the system administrator, security administrator, supervisors and department directors to access any e-mail system, files or communications that do not belong to them except for authorized business purposes or as noted in Section 7. The County reserves the right to monitor access in order to ascertain whether unauthorized access has been attempted.

12. Failure to comply:

Employees who fail to comply with this policy may be subject to disciplinary action that could result in cancellation of system access, disciplinary action up to and including termination of employment and/or criminal prosecution.

13. Policies specific to Internet access and usage:

a. Integrity of Information. When using information from an Internet site for County business decisions, employees should verify the integrity of that information, i.e., that the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information. Just because it is there does not mean that it is accurate or valid.

The County has no control or responsibility for content on an external server not managed by DTS.

b. Web-based Applications. The use of free web-based applications must be approved by DTS.

- Employees are responsible for any County content stored and must ensure that the information is protected and conforms to all County policies.

- Employees are responsible for ensuring that the County information that is used or posted is authorized to be released to the public and any content created by the user is retained in accordance with the County's record management policies. Both record retention and information security standards apply to non-county hosted Web sites.

- Sensitive or Confidential information requires pre-approval before posting or use in an web-based application and includes but is not limited to Personally Identifiable Health information (ePHI), dates of birth, Social Security Numbers (SSN); Critical Infrastructure (CI) information such as drinking water, sewage pipe, fiber, underground power grid routes, internal disaster recovery plans; and also includes but is not limited to information that in any manner that describes, locates or indexes anything about an individual including, but not limited to, his/her (hereinafter "his") real or personal property holdings, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, Social Security Number, tax status or payments, date of birth, address, phone number or that affords a basis of inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, and the record of his presence, registration, or membership in an organization or activity, or admission to an institution or other sensitive information and should not be content that is associated with free WEB based applications which often times retain or track the content.
- Free web tools that help develop presentation materials are not in the control of DTS are not authorized for use by employee

c. Commercial Internet accounts. All access to the Internet, for County purposes or on County equipment, will be provided through the County's Internet access facilities. Commercial subscription accounts (e.g., COMCAST, AOL, etc.) are not authorized.

d. Streaming media. Certain features of the Internet, such as streaming audio and video, can saturate the County's Internet connection, and are only to be used for County business.

e. File Transfer Protocol (FTP). A user should not FTP to any system on which they do not have an account, or that does not allow anonymous FTP services. Downloaded files may contain viruses. Observe the County's policy with respect to scanning files for viruses. Observe any posted restrictions on the FTP server.

f. Telnet. Users should not Telnet (a program that allows the user to access distant computers via TCP/IP connections) to machines on which they do not have an account, or where there is no guest account. Users should observe any posted restrictions when they Telnet to another machine.

g. Remote Access. Users who are authorized to Telework must use the DTS provided Remote Access (RA) method. Other remote access services are not authorized for use. Services such as "LOGMEIN," "GOTOMYPC," VNC, and Team Viewer, etc., are not under the control of DTS and thus have less than optimal security and are not permitted to be used in conjunction with County networked resources.

14. Electronic Communications:

Employees provided with County account(s) are to protect their account information by excluding unnecessary exposure of the County email address (not to be published in public media, newspapers, social media applications, websites, etc.). The account is for County business, subject to any limitations outlined in this policy. Electronic communications (e-mail, voice mail, social media, texting, etc.) are subject to the provisions of the Virginia Freedom of Information Act and Virginia Public Records Act and the requirements below:

a. Respond appropriately to messages and follow proper etiquette when fashioning email correspondence.

b. Be aware of email security best practices.

c. Ensure the e-communication is sent to the person/s for which it was intended by confirming that you have the correct contact information. Use the "reply all" feature carefully.

d. Respond appropriately to Freedom of Information Act (FOIA) requests.

e. Protect e-communications from unauthorized release to third parties. Sensitive information should be protected through encryption.

f. Utilize official County-issued accounts for communications regarding transaction of County business**.**

15. Records Management:

a. Management of Electronic Records

All public records created, stored, or received on County information systems are to be retained in accordance with the provisions of these guidelines and as described in the Virginia Public Records Act (§ 42.1-76 et seq.) and the Library of Virginia (LVA) Records Retention & Disposition Schedules. Additional guidance and policies regarding the management of county records can be found on the Records and Information Management site on AC Commons.

b. Retention of Electronic Communication Records

By default, records generated in electronic communication systems are retained as "Correspondence", under General Records Retention & Disposition Schedule 19 for localities. Electronic Communication systems include, but are not limited to, e-mail and social media applications.

Electronic Communication systems are not designed to be records management systems. Records other than routine "Correspondence" are not to be stored in electronic communications systems. All Arlington County staff members and contractors are responsible for ensuring that records are retained for the appropriate retention period pursuant to LVA requirements. **It is the responsibility of each staff member to determine if records require longer retention** by reviewing the appropriate LVA retention schedules and moving the record into a County approved records management system.

16. Related Information:

https://my.arlingtonva.us/pls/portal/docs/PAGE/AC_EMPLOYEE_BENEFITS/DOCUMENTS AND FORMS/AR 2.7 080306.DOC - _Toc148258624

Separate County policies address Security, Records Management, the County's web site and public Internet use through Libraries. These policies include (but are not limited to) the DTS Mobile Device Use and Management Policy, Administrative Regulations on Social Media Policy and Guidelines, Use of County Video Systems, and Records and Information Management.

Appendix E: Sample Nondisclosure and Data Security Agreement (Arlington County)

AGREEMENT NO. 281-10-1

EXHIBIT B

COUNTY NONDISCLOSURE AND DATA SECURITY AGREEMENT

I agree that I will hold County information, documents, data, images, records and the like (hereafter "Information") confidential and secure, and protect that Information against accidental loss, misuse, alteration, destruction, or disclosure. Information includes, but is not limited to, the information of the County, its employees, other contractors, residents, taxpayers, and property, and includes, but is not limited to, data that the County shares with Dimension Data, Inc. for testing, support, conversion, or for support services.

I agree that I will maintain the security of the Information and I will not divulge this Information or allow or facilitate access to it by any unauthorized person, for any purpose, or any information obtained directly, or indirectly, as a result of my participation on any Arlington County work. This Information includes, but is not limited to, information that in any manner describes, locates or indexes anything about an individual, including, but not limited to, his or her (hereinafter "his") real or personal property holdings, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, social security number, tax status or payments, or date of birth, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, and the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

I also agree that I will not directly or indirectly use or facilitate the use or dissemination of Information (whether intentionally or by inadvertence, negligence or omission) verbally, electronically, through paper transmission or otherwise, for any purpose other than that directly associated with my officially assigned duties on the Artisphere Management Software project. I am aware that any unauthorized use or disclosure of Information is prohibited and, in addition, may also constitute a violation of Virginia law (e.g., the Government Data Collection and Dissemination Practices Act, formerly called the Privacy Protection Act, Code of Virginia § 2.2-3800 et seq., and the Secrecy of Information Act, Code of Virginia § 58.1-3, which may be punishable by a jail sentence of up to six months and/or a fine of up to $1,000.00.)

I also agree that I will not divulge or facilitate the divulgence to or access by any unauthorized person of County confidential or proprietary Information obtained directly, or indirectly, as a result of my participation on any work performed for Arlington County. I also agree to view, retrieve or access such Information only to the extent concomitant with my assigned duties on the Project and only in accordance with the County’s and Dimension Data, Inc.’s access and security policies.

I also agree that I will take strict security measures and follow the County’s Information Security regulations to ensure that Information is not improperly stored, that if stored that it is encrypted and stored securely, and fully protected from retrieval or access by non-authorized persons, and that any device or media on which data is stored, even temporarily, will have strict security and access control, and that I will not cause any Information to leave my employer’s work site or the County’s physical facility, if working onsite. I also agree that I will not work remotely or remove any Information from my employer’s worksite or the County’s physical facility without express written authorization of the County’s Project Officer. If so authorized, I understand that I am responsible for the security of the Information and the electronic equipment or paper files on which the Information is stored. My signature below confirms that I have received and reviewed a copy of the County’s Information Security regulations”.

I will ensure that any hardware, laptop, other equipment or media connected to the County network shall be free of all of all computer viruses and/or running the latest version of an industry standard virus protection program. I will also ensure that my password, if any, is protected and not shared. No Information may be downloaded except as authorized by the County Project Officer and then only onto a County-approved device. Downloading onto a personally-owned device is prohibited.

I also agree that I will notify the County Project Officer immediately upon discovery or becoming aware or suspicious of any breach of this County Nondisclosure and Data Security Agreement, any County policy, access, my employer's security system, or any unauthorized use or disclosure of the Information, or any other breach of this County Nondisclosure and Data Security Agreement, and I will cooperate with the County in every way in any investigation to help the County regain possession of any Information, and to prevent its further unauthorized disclosure, use, or dissemination.

Name (print): ______________________________________

Signed: ____

Date: ____

Attest: ____

Date: ____

Appendix F: Sample Vendor Questionnaire (Arlington County)

Arlington County Information Governance Certification Requirements

Approved for Use
September 1, 2013
Revised June 12, 2014

Introduction

The Arlington County Project Proposal Matrix for Meeting Information Governance Policy Requirements is required as an attachment for information technology responses to Request for Proposal (RFP) or internal application development processes initiated by Arlington County Government. It is intended to assist Arlington County procurement with soliciting vendor responses that identify the requirements of the Arlington County Information Governance Policy. The clear identification of each element is required by Arlington County in order to sustain and ensure an adequate foundation for the development and implementation of secure information technology practices within Arlington County Government. Elements are included for issues relative to HIPAA Privacy, Security, and Records Management compliance in general.

This certification applies to all application data in transit, at rest, used and stored in support of government business. This certification also is required for any outsourced SaaS, CLOUD, or other off site data services in support of government business.

On-site vendors with access to Arlington County information resources are required to abide by all policies and procedures of Arlington County Government, Virginia.

How to Use the Security Template

The template is comprised of four sections:

1. Standard

This section includes the requirements to be addressed. Those requirements can take the form of a question or a statement.

2. Does Your System Comply?

The responder shall provide a high level response to the Standard. The answers can be YES, NO, or Alternative (ALT). The responder MUST check one of the three boxes to indicate their position or solution capability. If the ALT box is checked the responder must provide a high level explanation of the alternative in the “Comments/Plans for the Meeting Compliance” section. If there is supplemental information requested within the system compliance column, an answer MUST be provided.

3. Where in Your Proposal is the Solution Described?

In this section the responder shall insert the technical proposal reference to the details of the solution. It should be specific (e.g., volume, chapter/section, page and paragraph heading) as to where the answer can be found. Failure to provide the reference or an incorrect reference shall be considered a NO answer. The correct reference location will not be researched by the procurement office or other Arlington County Departments.

4. Comments/Plans for Meeting Compliance

In this section the responder may provide any high level comments that may clarify a response in the "Does System Comply" section. It is especially important for responders to use this section to explain alternative checked responses. An alternative response can include a statement of future development or a solution that addresses the requirement, however may not be a direct answer/solution to the requirement. This section MUST NOT be used for detailed descriptions of the response.

References:

This template was based upon similar work approved for public distribution by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) in August 2003; modified for Arlington County Government, February 2013.

	STANDARDS	SYSTEM SPECIFICATIONS?	WHERE IN YOUR PROPOSAL IS THE SPECIFICATION DESCRIBED?
	A. Description		
A.1.	**System Name/Title:**		
A.2.	**Vendor/Developer:**		
A.3.	**RFP Reference Number:**		
A.4.	**Application Type:**	COTS:□ Proprietary: □ ALT: □ .NET □ JAVA □ OTHER □ explain: _________ ___________	
A.5.	**Provide a copy or statement about your software development life cycle standards and approach.**		
A.6.	**Database Requirements:**	Yes:□ No: □ ALT: □ □ Oracle 10G or higher □ DB2 Release 7 □ Microsoft SQL Server 2005 □ Other	
A.7.	**User access controls are:**	□ Built into the system **(Must respond to Sections A, B, C, D, E, & F)** □ Standard operating system **(Must respond to Sections A, C, D, E, & F)** □ Active Directory □ LDAP □ RACF □ Database control **(Must respond to Sections A, C, D, E, & F)** □ Oracle □ DB2 □ SQL	

		□ Other **(Must respond to Sections A, B, C, D, E, & F)**	
A.8	**List all additional system components required to make the proposed solution work, including any applets and/or plug-ins.**		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	B. Password controls			
B.1.	**System enforced: specified strong password to include minimum length and combination of alpha and numeric characters**	Yes:□ No: □ ALT: □ Current Minimum: ___ Current Maximum: ___		
B.2.	**System enforced: user passwords automatically changed or revoked after a user defined period has passed**	Yes:□ No: □ ALT: □ Current Change Interval: ___		
B.3.	**System enforced: users required to change their passwords following the initial set up or resetting of the password**	Yes:□ No: □ ALT: □		
B.4.	**System enforced: system administrators may not disable password controls**	Yes:□ No: □ ALT: □		
B.5.	**System prevents auto logon, application remembering, embedded scripts, and hard-coded passwords in software**	Yes:□ No: □ ALT: □		
B.6.	**History of previously used passwords is maintained by the system to prevent reuse**	Yes:□ No: □ ALT: □ Current Value: ___		
B.7.	**Users are provided the capability to change their own passwords at their discretion**	Yes:□ No: □ ALT: □		
B.8.	**User id's are disabled after a specified number of consecutive invalid login attempts**	Yes:□ No: □ ALT: □ Current # Attempts: ___		
B.9.	**System automatically activates a password protected screensaver when units remain idle for determined period of time**	Yes:□ No: □ ALT: □		
B.10.	**System automatically logs users off after a specified period of inactivity**	Yes:□ No: □ ALT: □ Current Auto logoff Time:___		

B.11.	**Passwords entered in a non-display field**	Yes:□ No: □ ALT: □		
B.12.	**Passwords encrypted when routed over a network**	Yes:□ No: □ ALT: □		
B.13.	**Passwords are encrypted in storage**	Yes:□ No: □ ALT: □		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	C. Security Administration			
C.1.	**System logs unauthorized access attempts by date, time, user id, device and location**	Yes:□ No: □ ALT: □		
C.2.	**System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:□ No: □ ALT: □		
C.3.	**System provides security reports of users and access levels**	Yes:□ No: □ ALT: □		
C.4.	**System provides a field(s) for personal information to be used for verification of users' identities for password resets and other maintenance (i.e., Mother's Maiden Name, DOB, etc.). Fields used would not be a requirement**	Yes:□ No: □ ALT: □		
C.5.	**System provides varying levels of access within the security application (i.e. access to only password reset functions or access to password reset function +Access to add & update users)**	Yes:□ No: □ ALT: □		
C.6.	**System permits the assignment of designated Access Control Administrators**	Yes:□ No: □ ALT: □		
C.7.	**System provides varying levels of access within the application**	Yes:□ No: □ ALT: □		
C.8.	**System uses groups and unique user ids to define levels of access**	Yes:□ No: □ ALT: □		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	C. Security Administration (continued)			
C.9.	**System provides the capability to place security controls on each system module and on confidential and critical levels within each module**	Yes:☐ No: ☐ ALT: ☐		
C.10.	**System provides capability to restrict access to particular records within the system, based on user id**	Yes:☐ No: ☐ ALT: ☐		
C.11.	**System provides capability of encryption of confidential or sensitive information stored locally on the device**	Yes:☐ No: ☐ ALT: ☐		
C.12.	**System provides capability of encryption of confidential or sensitive information transmitted over the network**	Yes:☐ No: ☐ ALT: ☐		
C.13.	**On-site training and sufficient supporting reference materials related to security administration for system administrators are provided prior to migration of product to production environment**	Yes:☐ No: ☐ ALT: ☐		
C.14.	**System provides centrally managed updates to protect against vulnerabilities**	Yes:☐ No: ☐ ALT: ☐		
C.15	**System will operate as described in conjunction with the County's chosen Anti-virus, anti-malware, and anti-spam protection software.**	Yes:☐ No: ☐ ALT: ☐		
C.16	**If this system stores PII, PPI or HIPAA data has the County Privacy Officer (HR Director) approved the Business Associate Agreement (BAA)?**	Yes:☐ No: ☐ ALT: ☐		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	D. Activity Logging			
D.1.	**System logs unauthorized access attempts by date, time, user id, device and location**	Yes:□ No: □ ALT: □		
D.2.	**System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:□ No: □ ALT: □ Number of days kept: ——		
D.3.	**System logs all inquiry accesses to data**	Yes:□ No: □ ALT: □		
D.4.	**System logs all modification accesses to data**	Yes:□ No: □ ALT: □		
D.5.	**System has auditing capabilities for both online or batch reporting. Can also be exported into County standard databases**	Yes:□ No: □ ALT: □		
D.6.	**Can logs be archived and recalled as needed?**	Yes:□ No: □ ALT: □ Archive methods: □ Tape □ Disk □ Other		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	E. Networking and Compatibilities			
E.1.	**Provide a diagram of the recommended network connectivity, interfaces, and data exchanges required for the proposed solution. Include a description and any additional explanation necessary to explain the method of interaction (e.g., read/write, synchronous/ asynchronous).**			
E.2.	**System configuration/architecture (i.e., hardware, wiring, display, network, and interface) is documented and included in proposal.**	Yes:□ No: □ ALT: □		
E.3.	**Does your solution support external data transmission? Please indicate the method(s) supported.**	Yes:□ No: □ ALT: □ Methods: □ Secure FTP □ Fax □ Email □ File Copies (CD, Diskette, etc.) □ Browser applications □ Tape media □ Web services □ Other:		
E.4.	**For externally electronically transmitted information, can the solution support encryption and data protection?**	Encryption: Yes:□ No: □ ALT: □ Data Protection: Yes:□ No: □ ALT: □		
E.5.	**For wireless transmission of data, does the system support the Arlington County wireless standards?**	Yes:□ No: □ ALT: □		

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	E. Networking and Compatibilities (continued)			
E.6.	**Can the system be accessed remotely (i.e., Internet, etc.). If applicable, provide an explanation of your wireless transmission requirements for the proposed solution.**	Yes:□ No: □ ALT: □ Methods: □ Dialup □ Internet □ Internet VPN □ Wireless		
E.7.	**For management and vendor support can the system support secure remote access (VPN/Dual Factor Authentication)?**	Yes:□ No: □ ALT: □ Methods: □ Security tokens that provide one-time password authentication □ Public/Private keys with strong pass phrases □ Citrix		
E.8.	**What anti-virus and end-point security software is the proposed solution compatible with? Provide version details with answer.**			

	STANDARDS	DOES SYSTEM COMPLY?	WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?	COMMENTS/PLANS FOR MEETING COMPLIANCE
	F. Contingency, Continuity, & Back-up			
F.1.	**What is your back up policy for the proposed solution?**			
F.2.	**For vendor supported, maintained, and managed solutions is there a Business Continuity Plan and a Disaster Recovery Plan?**	Yes:☐ No: ☐ ALT: ☐ ☐ Not applicable, County supported		
F.3.	**Does your solution automatically monitor database capacity requirements to reduce the risk of system overload? If yes, is a warning alert provided to the system administrator?**	Yes:☐ No: ☐ ALT: ☐ ☐ Warning alert provided ☐ Not applicable, County supported		
F.4.	**In the event of an identified vulnerability to or within the system, are there designated technical support personnel available to assist Arlington County with eliminating or mitigation of the vulnerability?**	Yes:☐ No: ☐ ALT: ☐ ☐ Not applicable, County supported		
F.5.	**In the event of an identified vulnerability will there be a zero-day vendor response team assigned to provide support to Arlington County IT administrator(s)?**	Yes:☐ No: ☐ ALT: ☐		
F.6	**In the event of an incident or hardware/software fault does the application support redundant auto-failure, i.e. seamlessly transition the application to the redundant platform?**	Yes:☐ No: ☐ ALT: ☐		
	G. Records Retention			

G.1.	Please describe (in detail) the type of information to be stored in the proposed system	Yes:□ No: □ ALT: □		
G.2.	Are you aware of existing records retention requirements for the content (See Virginia Records Retention Requirements If yes, please state the requirements.	Yes:□ No: □ ALT: □		
G.3.	Are you proposing to store any Personally Identifying Information in the system (SSN, Driver's License, financial information, etc.)? If so, please describe the business need and safeguards in place to secure the information.	Yes:□ No: □ ALT: □		
G.4.	Does the system allow for records to be protected from unauthorized modification or deletion?	Yes:□ No: □ ALT: □		
G.5.	Does the system allow for records to be tagged (classified) and assigned a retention policy/schedule ensuring that the record is retained pursuant to the policy?	Yes:□ No: □ ALT: □		
G.6.	Does the system allow for automated destruction/deletion of records that have met or exceeded the required retention schedule?	Yes:□ No: □ ALT: □		

G.7.	**Does the system allow for automated destruction to be suspended in the event of anticipated litigation and/or investigation (legal hold)?**	**Yes:□ No: □ ALT: □**		
G.8.	**Does the system allow for retrieval and production of information for e-discovery and FOIA compliance?**	**Yes:□ No: □ ALT: □**		
G.9.	**If the system does not contain any of the required functions identified in G.4. – G.8., have you ensured that it integrates with county systems that do contain the required functionality? If yes, please describe your solution.**	**Yes:□ No: □ ALT: □**		
	H. Data Security/Privacy			
H.1.	**If this system stores HIPAA or PII data is the data secured through encryption?**	Yes:□ No: □ ALT: □		
H.2.	**If this system is capable of utilizing GPS for tracking purposes has Terms and Conditions of use language been prepared?**	Yes:□ No: □ ALT: □		
H.3.	**If this is a public facing application and GPS is potentially part of the offering has a straw man education and promotion package been prepared?**	Yes:□ No: □ ALT: □		

Appendix G: Specifications for Network Shelters

Installed shelters and related subcomponents shall meet these minimum specifications:

- Compliance with national and local codes:
    - Interior dimensions of at least 10 feet (width) x 12 feet (length) x 10 feet (height)
    - Structural walls and ceiling components consisting of precast, minimum 5000 PSI, steel reinforced concrete
    - Support a floor equipment load of minimum 500 PSF
    - Support a roof live load of 100 PSF
    - Building code-recognized fire rated for 2 hours
    - Withstand wind speeds of 150 mph when secured to proper foundation
    - Bullet resistance per UL752, Level 4 (.30-06 at 15 feet)
    - Foundation comprised of a level, concrete pad with steel reinforcement
    - Two underground cable entry points for communications cable shall be provided, each equipped to support two 2-inch conduits

- Interior finishing and cable accessory specifications:
    - One wall-mounted, painted plywood board (4 ft. x 4 ft. x ¾-inch thick) for telecommunications and other wall-mounted equipment
    - Cable ladders having a width of 12-inches and a total length of approximately 22 feet ceiling/wall mounted to provide 8 feet of clearance to the floor

- Cooling and heating system specifications:
    - Two 5-ton (redundant), self-contained HVAC units with 5 kW heat strips be wall-mounted to the shelter, designed to be weather-proof, rodent-proof, and tamper-proof
    - Each HVAC unit fed from separate circuit breakers in the main distribution panel

- Electrical system specifications:
    - Main distribution load center providing a minimum of 20 positions, consisting of the main distribution panel, breakers, lug box, and related components for 200A, 120/240v, single phase electrical service
    - UL 1449 Type 1 SAD/MOV surge protection
    - Minimum of four duplex, 20 Amp wall-mounted receptacles
    - 35 kW diesel electrical generator
        - Minimum 140-gallon sub-base fuel tank
        - Automatic transfer switch

- Lighting specifications:
    - 4-foot, two bulb fluorescent fixtures with acrylic lens covers (minimum four)
    - 150-watt exterior lighting fixture with photo-cell and motion sensor control

- Alarms and fire protection systems:
    - High temperature
    - Low temperature
    - Generator
    - Air conditioner failure
    - Primary power failure
    - Door opened/closed
    - Fire and smoke alarm
    - Inert gas fire suppression system (FM-200, or equivalent)

Appendix H: Sample Internal Operating Procedures (Arlington County)